

3
avf
5-18-01

Docket No.: 58'99-031

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Koichi YONETA, et al.

Serial No.:

Group Art Unit:

Filed: February 02, 2001

Examiner:

For: DIGITAL INFORMATION SALES METHOD

11036 U.S. PTO
09/773905
02/02/01

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-115781,
filed April 11, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty

Michael E. Fogarty
Registration No. 36,139

Larry T. Callen
Ly: 44,489

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:klm
Date: February 2, 2001
Facsimile: (202) 756-8087

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

McDermott, Will & Emery

5450 FEBRUARY 6, 2001
YONSTRA et al.

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2000年 4月11日

出願番号
Application Number:

特願2000-115781

出願人
Applicant(s):

株式会社日立製作所
株式会社日立画像情報システム

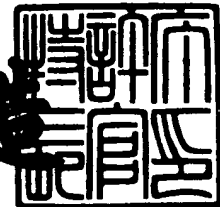
J1036 U.S. PTO
09/773905
02/02/01

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月22日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3106239

【書類名】 特許願

【整理番号】 D99007291A

【提出日】 平成12年 4月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明の名称】 デジタル情報販売方法及びデジタル情報販売装置

【請求項の数】 13

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
画像情報システム内

【氏名】 米田 幸一

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
画像情報システム内

【氏名】 井上 雅之

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
画像情報システム内

【氏名】 名波 秀昇

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
画像情報システム内

【氏名】 稲光 哲治

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
画像情報システム内

【氏名】 佐藤 勝俊

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立

製作所デジタルメディア開発本部内

【氏名】 伊藤 滋行

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア開発本部内

【氏名】 高見 穰

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア開発本部内

【氏名】 松本 健司

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区吉田町 2 9 2 番地 株式会社日立
製作所デジタルメディア開発本部内

【氏名】 井上 喜勇

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【特許出願人】

【識別番号】 000233136

【氏名又は名称】 株式会社 日立画像情報システム

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

特 2 0 0 0 - 1 1 5 7 8 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル情報販売方法及びデジタル情報販売装置

【特許請求の範囲】

【請求項 1】

デジタル情報を販売する方法であって、

前記デジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第 1 の記憶媒体から、デジタル情報制御装置を用いて第 2 の記憶媒体へキー情報を複製する際に、記憶媒体所有者がアクセスできない販売者エリアへデジタル情報を利用するための料金を格納させるようにデジタル情報制御装置を制御するプログラムと、

をデジタル情報の販売の際に、第 1 の記憶媒体に記憶させることを特徴とするデジタル情報販売方法。

【請求項 2】

デジタル情報を販売する方法であって、

前記デジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第 1 の記憶媒体から、デジタル情報制御装置を用いて第 2 の記憶媒体へキー情報を複製する際に、記憶媒体の記憶媒体所有者がアクセスできない販売者エリアへデジタル情報を利用するための料金を格納させる機能と、

前記記憶媒体を用いて通信を行うときに、前記販売者エリアに格納された料金を販売元へ送信するようにデジタル情報制御装置を制御する機能を有するプログラムと、

をデジタル情報の販売の際に、第 1 の記憶媒体に記憶させることを特徴とするデジタル情報販売方法。

【請求項 3】

前記プログラムは、前記第 $N - 1$ の記憶媒体 (N は 3 以上の整数) から、第 N の記憶媒体へ前記キー情報を複製する際にも、記憶媒体の記憶媒体所有者がアクセスできない販売者エリアへデジタル情報を利用するための料金を格納させるようにデジタル情報制御装置を制御する機能を有することを特徴とする請求項

1 又は 2 に記載のデジタル情報を販売する方法。

【請求項 4】

前記プログラムは、前記第 N の記憶媒体の前記販売者エリアに前記利用料金を格納するように制御する機能を有することを特徴とする請求項 3 に記載のデジタル情報を販売する方法。

【請求項 5】

前記プログラムは、前記第 N の記憶媒体と、前記第 N - 1 の記憶媒体の、販売元との取り引き回数を比較し、取り引き回数の多い記憶媒体の前記販売者エリアに前記利用料金を格納するように制御する機能を有することを特徴とする請求項 3 に記載のデジタル情報を販売する方法。

【請求項 6】

前記プログラムは、前記販売者エリアに利用購入金額を有する記憶媒体が A T M 装置に挿入されたときに、前記販売者エリアに格納された金額情報をデジタル情報販売装置へ送信させるように、前記 A T M を制御する機能を有することを特徴とする請求項 1 乃至 5 のいずれかに記載のデジタル情報を販売する方法。

【請求項 7】

デジタル情報を販売する方法であって、

前記デジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第 1 の記憶媒体から、第 2 の記憶媒体へキー情報をデジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該デジタル情報制御装置を制御する機能を有するプログラムと、

をデジタル情報の販売の際に、第 1 の記憶媒体に記憶させることを特徴とするデジタル情報販売方法。

【請求項 8】

デジタル情報を販売する方法であって、

前記デジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第 1 の記憶媒体から、第 2 の記憶媒体へキー情報をデジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で

複製されるように、該デジタル情報制御装置を制御する機能と、

複製されたデジタル情報の再生する際に、前記第 2 の記憶媒体に記憶されたキー情報を使用可能な状態にするために、通信手段によりデジタル情報販売元にアクセスさせるようにデジタル情報制御装置を制御する機能とを有するプログラムと、

をデジタル情報の販売の際に、第 1 の記憶媒体に記憶させ

使用不可の状態のキー情報が記憶された第 2 の記憶媒体を用いてアクセスがあったときに、前記デジタル情報の利用料金を支払いにより、前記第 2 の記憶媒体に記憶されたキー情報を使用可能な状態させる情報を送信することを特徴とするデジタル情報の販売方法。

【請求項 9】

デジタル情報を記憶する記憶手段と、

前記デジタル情報の利用許可を示すキー情報を記憶する手段と、

前記デジタル情報と前記キー情報を購入することにより前記キー情報が書きこまれた第 1 の記憶媒体から、第 2 の記憶媒体へ、前記キー情報をデジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該デジタル情報制御装置を制御する機能を有するプログラムを格納する手段とを有し、

該デジタル情報の販売の際に、前記キー情報と前記プログラムを購入者の記憶媒体に記憶させることを特徴とするデジタル情報販売装置。

【請求項 10】

デジタル情報を記憶する記憶手段と、

前記デジタル情報の利用許可を示すキー情報を記憶する手段と、

前記デジタル情報と前記キー情報を購入することにより前記キー情報が書きこまれた第 1 の記憶媒体から、第 2 の記憶媒体へ、前記キー情報をデジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該デジタル情報制御装置を制御する機能と、複製されたデジタル情報の再生する際に、前記第 2 の記憶媒体に記憶されたキー情報を使用可能な状態にするために、通信手段によりデジタル情報販売元にアクセスさせるようにディ

タル情報制御装置を制御する機能とを有するプログラムを格納する手段とを有し

該デジタル情報の販売の際に、前記キー情報と前記プログラムを購入者の記憶媒体に記憶させ、

該第 2 の記憶媒体を用いてアクセスがあったときに、前記デジタル情報の利用料金を支払いにより、前記第 2 の記憶媒体に記憶されたキー情報を使用可能な状態させる情報を送信することを特徴とするデジタル情報販売装置。

【請求項 1 1】

デジタル情報の利用許可を示すキー情報が格納された第 1 の媒体を制御する手段と、

第 1 の媒体に記憶された該キー情報を第 2 の媒体へ複製する手段を有するデジタル情報制御装置を制御する機能を有する制御装置が読み取り可能なプログラムであって、

前記制御装置に、前記第 1 の媒体に記憶されたキー情報を、前記第 2 の媒体へ複製する際に、前記キー情報を使用不可の状態にさせ、使用不可状態のキー情報を第 2 の媒体に記憶させる機能を実現させることを特徴とするプログラム。

【請求項 1 2】

デジタル情報の利用許可を示すキー情報が格納された第 1 の媒体を制御する手段と、

第 1 の媒体に記憶された該キー情報を第 2 の媒体へ複製する手段と、

複製されたキー情報が格納された第 2 の媒体を制御する手段と、

外部装置と通信可能な通信手段とを有するデジタル情報制御装置を制御する機能を有する制御装置が読み取り可能なプログラムであって、

前記制御装置に、

前記第 1 の媒体に記憶されたキー情報を、前記第 2 の媒体へ複製する際に、前記キー情報を使用不可の状態にさせ、使用不可状態のキー情報を第 2 の媒体に記憶させる機能と、

複製されたデジタル情報を再生する際に、前記第 2 の媒体を用いて前記通信手段により、デジタル情報の販売装置へ通信を行わせることにより、前記第 2

の媒体に記憶された使用不可状態のキー情報を使用可能な状態にする機能を実現させることを特徴とするプログラム。

【請求項 1 3】

前記第 1 の記憶媒体と第 2 の記憶媒体は、電子マネー情報と、ＩＣカード固有のキー情報を有するＩＣカードであり、前記キー情報が第 1 の記憶媒体又は第 2 の記憶媒体に記憶される際に、該ＩＣカード固有のキー情報により暗号化されていることを特徴とする請求項 1 乃至 8 のいずれかに記載のデジタル情報の販売方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル情報の販売・管理システム及び装置に関する。

【0 0 0 2】

【従来の技術】

デジタル情報の最大の特長はデータの劣化がないことである。そこで、利用者間におけるデジタル情報の不正な複製及びその利用、又はその複製したデジタル情報の販売などが深刻な問題となっている。このデジタル情報の管理する方法の一例として、特公平 6 - 2 8 0 3 0 号「ソフトウェア管理方式」（以下、ソフトウェア管理方式という）が挙げられる。

【0 0 0 3】

【発明が解決しようとする課題】

デジタル情報の正当な利用方法の提供に際して、権利者と利用者、又は利用者間を伝達、又は複製されるデジタル情報には何らかのセキュリティ保護が必要であると考えられる。

【0 0 0 4】

上記ソフトウェア管理方式では、有償データ固有の情報を規定のメモリに記憶していることを条件に、ソフトウェアの利用を許可する。しかし、利用条件である有償データ固有の情報を各利用者の規定のメモリにコピーすれば、ソフトウェアの利用が可能になってしまう。特に、利用者間において、上記コピーが行われ

ると、そのソフトウェアはフリーソフトのごとく無償で利用されてしまう恐れがあり、権利者が受け取るべき料金が回収できなくなる危険性がある。

【0005】

また、上記ソフトウェア管理方式では、払戻しのインセンティブにより、外部入出力処理部にて利用明細情報の報告を行うことを利用者に促すことで協会が利用明細を取得し、協会から明細の内容に合致した金額を権利者の銀行口座に振り込むことで、利用者から権利者への料金回収を実現している。しかし、通信機能を利用した利用明細の報告を行う場合、すべての利用者に通信機能が必要であるという限定がかかり、利用者に対して設備投資の負荷がかかってしまう。また、利用者間の複製ではオフライン環境下でしか稼働できないような端末での利用も考えられ、オフライン環境下の利用者への拡販が見込めないことになる。

【0006】

【課題を解決するための手段】

そこで、本発明では、映像、音楽、著書などのデジタル情報の販売・管理を行うために、セキュリティ保護されたデジタル情報を、利用者間で利用又は複製することを可能とし、デジタル情報の利用に伴う料金をデジタル情報の権利者へ確実に回収できる方法を提供する。

【0007】

デジタル情報のセキュリティ保護を行うために、デジタル情報を再生するためのキー情報を設け、キー情報に基づき、デジタル情報の再生を判断する。このキー情報の複製の際に、以下の2つの方法により、セキュリティの担保と料金回収を達成する。

第1の方法は、デジタル情報とキー情報の複製の際に、ユーザーがアクセスできない販売者エリアに販売金額を格納させることとする。この方法によれば、デジタル情報を複製したユーザーは、オフラインでデジタル情報を複製した場合であっても、キー情報が上記第1の方法と異なり使用可能であるため、デジタル情報を利用することができる。また、販売者エリアに格納された料金を後日、オンラインや銀行ATM等により、回収することができるため、オフラインで複製した場合であっても料金を回収することができる。

【 0 0 0 8 】

第2の方法は、として、正規の利用者ではない他の利用者がデジタル情報を複製するときは、キー情報を使用不可の状態で複製させる。デジタル情報の複製時には、キー情報が使用不可となっているため、キー情報をコピーしてもデジタル情報を利用できない。したがって、不正な複製による利用を阻止することができる。そして、デジタル情報を複製した利用者は、デジタル情報を利用する際に、販売元へアクセスして料金を支払い、使用不可のキー情報のロックを解除する。デジタル情報の利用に際して、必ず販売元へアクセスするので、このときに料金を確実に回収することができる。

【 0 0 0 9 】

なお、複製の際や回収の際にこのような制御を行わせるためのプログラムを、デジタル情報、キー情報と共に、利用者の記憶媒体に記憶させて、デジタル情報を販売することとする。

【 0 0 1 0 】

【発明の実施の形態】

本発明の第1の実施例を、図1から図4を用いて説明する。第1の実施例は、デジタル情報の利用に際してキー情報が必要であり、デジタル情報とキー情報の複製の際に、ユーザーがアクセスできない販売者エリアに販売金額を格納させるものである。

【 0 0 1 1 】

図1に、本発明が適用される有料デジタル情報の購入、転売及びその料金回収方法に関するシステムの一実施例の構成図を示す。図2に、本システムにおける著作権権利者とデジタル情報を購入する第一利用者間のデジタル情報販売手順を示す。図3に、第一利用者が購入したデジタル情報を利用するための手順を示す。図4に、第一利用者と著作権権利者から直接デジタル情報の購入をしていない第二利用者間の複写手順を示す。

【 0 0 1 2 】

図1において、デジタル情報販売装置1はデジタル情報を販売する著作権権利者や販売者の端末である。デジタル情報2は著作権権利者又は販売者（以

下、販売元という) 固有の情報で暗号化された映像、音楽又は著書などである。暗号化情報生成器 3 はデジタル情報を販売元固有の情報で公開かぎ方式や共通かぎ方式などの暗号方式により対象データを暗号化する。販売元所有の I C カード(以下、販売元カードという) 4 は、販売元固有の情報や電子マネー情報が少なくとも格納されている。販売元 I C カード制御装置 5 は販売元カード 4 の情報を読み書きするためのもので、通常、販売元カード 4 がこの販売元カード制御装置 5 に装着されているものとする。利用者所有の I C カード(以下、利用者カードという) 6 は、利用者固有の情報や電子マネー情報が格納されている。利用者カード制御装置 7 は、デジタル情報販売装置 1 に内蔵されており、利用者カード 6 の情報の読み書き制御を行う。デジタル情報を利用者が購入する場合、この利用者カード制御装置 7 に利用者カード 6 を装着する。販売履歴メモリ 8 はデジタル情報の販売履歴の情報を記憶するためのものであり、販売したデジタル情報の名称、利用者カード固有の情報などを格納する。販売者側外部通信手段 9 は、デジタル情報販売装置 1 と外部機器との通信を行うためのものであり、直接又は間接適に利用者所有の装置と接続かつ通信することが可能である。販売者側プログラム記憶手段 1 0 は、デジタル情報販売装置を構成する各手段を制御するため必要なプログラム情報を格納するためのものであり、電子マネー情報を利用した決済を制御するプログラムなどが格納されている。販売者側外部入出力手段 1 1 はデジタル情報販売装置 1 の処理結果の表示などを外部へ出力するための出力機能や、デジタル情報販売装置 1 の処理を実行するために外部からキーなどの情報を入力するための入力機能を備えている。販売者ユニット制御手段 1 2 はデジタル情報販売装置 1 を構成する各手段、暗号化情報生成器 3、販売元カード制御装置 5、利用者カード制御装置 7 等を制御する。デジタル情報 2 は、利用者が所有するデジタルデータ格納媒体 2 3 に記憶される。なお、デジタル情報 2 はデジタル情報販売装置内の、不図示の記憶手段に記憶されている。

【 0 0 1 3 】

デジタル情報制御装置 1 3 は利用者が購入したデジタル情報を表示又は音声などにより利用するため装置である。暗号化情報再生器 1 4 は、暗号化されたデジタル情報を利用するために必要な複合処理を行う。第 1 利用者カード制御

装置 1 5 は、第 1 利用者カード制御装置に内蔵され、利用者カード 6 の情報に対して読み書き制御を行う。第 2 利用者カード制御装置 1 6 は、利用者カードの情報に対して読み書き制御を行う。デジタル情報格納媒体制御装置 1 7 は、デジタル情報を格納した記憶媒体 2 3 を装着して、この媒体からデジタル情報を読み出す。1 8 はデジタル情報制御装置固有の情報を格納するためのデジタル情報制御装置情報記憶手段である。利用者側プログラム記憶手段 1 9 はデジタル情報制御装置を構成する各手段を制御するために必要なプログラム情報を格納する。デジタル情報再生手段 2 0 は、複合化されたデジタル情報の表示、出力などを行う。利用者側入出力手段 2 1 は、デジタル情報制御装置 1 3 の処理結果の表示などを行うための出力機能を備え、また、デジタル情報販売装置 1 の処理を実行するために、外部からキーなどの情報を入力するための入力機能を備える。販売者ユニット制御手段 2 2 は、デジタル情報制御装置を構成する各手段、暗号化情報再生器 1 4、第 1 利用者カード制御装置 1 5、第 2 利用者カード制御装置 1 6 等を制御する。利用者側外部通信手段 2 3 はデジタル情報制御装置 1 3 と外部機器との通信をするためのものであり、直接又は間接適に利用者所有の装置との通信が可能である。

【 0 0 1 4 】

なお、販売者側プログラム記憶手段 1 0 には、利用者へ秘密かぎ情報を販売するときに利用者の記憶媒体へ格納する秘密かぎ制御プログラムが格納されている。秘密かぎ情報制御プログラムは、秘密かぎの複製の制御や、販売者エリアからの利用料金の回収などを制御するものであり、デジタル情報制御装置 1 3 においても機能するものである。

【 0 0 1 5 】

図 2 に、販売元と第 1 利用者との販売手順を示す。第 1 利用者がデジタル情報販売装置 1 が設置されているデジタル情報販売店で、デジタル情報を購入する際の、主にデジタル情報販売装置 1 の処理動作を述べる。なお、図 2 には示していないが、利用者が販売を希望するデジタル情報 2 を、第 1 利用者所有の記憶媒体 2 3 に格納させる。これは、次に述べる料金の支払い前や秘密かぎ情報（キー情報）の格納前に行ってもよいが、料金支払い後や秘密かぎ情報の格納

後が好ましい。

【0016】

まず、第1利用者が所有する利用者カード（以下、第1利用者カードという）をデジタル情報販売装置1内蔵の利用者カード制御装置7に装着する。

第1利用者のデジタル情報記憶媒体販売者ユニット制御手段12は利用者カード制御装置7からカード挿入を示す情報を取得して（200）、販売するデジタル情報の料金に相当する電子マネー情報を第1利用者の利用者カードから徴収する（201）。この電子マネー決済では利用者カードから販売元カードへ上記の電子マネーが移動することになり、利用者カードに格納される電子マネーが減算され、販売元カードに格納される電子マネーが加算される。ただし、この電子マネーの加減算については、単にデータの読み出しとその値に対する加減算を行うのではなく、販売者側プログラム格納メモリ10に記憶される電子マネー制御プログラム及び利用者カードと販売元カードに内蔵されて記憶されている同電子マネー制御プログラムにより、プロトコル、通信データの暗号処理、また、販売元カードと利用者カード固有の情報を利用した認証処理を行い、セキュリティを担保させる。

【0017】

更に、図示していないが、第1利用者カードの電子マネーが記憶されているエリアを、第1利用者が使用できる電子マネー格納エリアと販売元に使用が限定される電子マネー格納エリアに分割する。この販売元にのみ使用が限定される電子マネー格納エリアは、後述の利用者間でのデジタル情報のやりとりの際、デジタル情報の購入料金として徴収する電子マネー情報を管理するために作成される。

【0018】

利用者カードより販売元カードへのデジタル情報購入料金の徴収が完了した場合（201-yes）、利用者カードから第1利用者固有の情報を取得する（202）。この時、デジタル情報の販売履歴を管理するために上記販売履歴メモリ8へ、取得した第1利用者の情報とデジタル情報の情報（例えば、デジタル情報登録名、販売価格、販売日時、購入者名、購入者ICカード番号など）

を関係付けして格納する。この情報管理により購入者からのクレームの対応や販売実績、又は購入者の傾向などを解析、管理することができる。また、ここでは第1利用者の秘密かぎ情報により復号化可能な暗号化の基になる情報（以下第1利用者暗号化情報）を少なくとも取得することにする。第1利用者暗号化情報は、利用者毎、あるいはカード毎に異なる情報であり、例えば、Purse ID (Personal ID) 等の情報である。

【0019】

次に、取得した第1利用者暗号化情報を基に、デジタル情報を復号化するために必要な販売元固有の秘密かぎ情報を暗号化する。この暗号化処理は販売者ユニット制御手段12から第1利用者暗号化情報と販売元固有の秘密かぎ情報を暗号化情報生成器3に渡し、暗号化情報生成器3により、販売元固有の秘密かぎ情報を暗号化する（203）。このような処理を行うことにより、デジタル情報を利用するための販売元固有の秘密かぎ情報が第1利用者固有の情報に基づいて暗号化されているため、暗号化されたデジタル情報が複製され、更に、暗号化された販売元固有の秘密かぎ情報が利用者カード以外の利用者カードに複写されたとしても、販売元固有の秘密かぎ情報は第1利用者暗号化情報を有しない利用者カードを使用しても複号化できない。従って、デジタル情報の不正な複製による使用を制限することができる。

【0020】

また、このとき、利用者間における販売元固有の秘密かぎ情報の複写の際の制御や、販売者エリアの料金の回収を行う秘密かぎ情報制御プログラムを、利用者カードに併せて書き込む。

【0021】

続いて、この暗号化情報生成器により暗号化した販売元固有の秘密かぎ情報を利用者カード制御装置7を用いて第1利用者カード6内部に書き込み（204）、第1利用者が希望するデジタル情報の販売処理を終了する。デジタル情報の販売処理において、購入者への操作の手順などを上記販売者側外部入出力手段11にディスプレイを接続して表示したり、購入者が不正なICカードを利用した場合などのエラー処理を同じように販売者側外部入出力手段11へスピーカー

を接続して、販売元及び購入者に通知するようにしても良い。

【0022】

また、上述の例においては、決済を電子マネーにより実施する形態を説明したが、紙幣、硬貨などの現金で支払いを行ってもよい。

【0023】

次に、図3を用いて、第1利用者が購入したデジタル情報を利用する場合の手順を説明する。

まず、販売元より上記で説明した手順により購入した、デジタルデータ格納媒体23に記憶されたデジタル情報2を、利用者のデジタル情報制御装置13に内蔵されるデジタル情報格納媒体制御装置17に装着する。デジタルデータ格納媒体23をデジタル情報格納媒体制御装置17に装着すると、利用者ユニット制御手段22でデジタル情報が装着されたことを検出する(300)。このデジタル情報の装着状態の検出や以下に記述する処理については、利用者側プログラム格納メモリ19に記憶されるユニット制御プログラムによって制御される。

【0024】

次に、デジタル情報からデジタル情報制御装置13を介してデジタル情報固有の情報(ここでは、ID番号1700とする。)を取得する(301)。この取得したID番号は暗号化されている情報である。デジタル情報の装着状態とID番号の取得が完了すると第1利用者カード制御装置15又は第2利用者カード制御装置16へ利用者カードが装着されているかを判定する。第1利用者カードには、上述の暗号化された販売元固有の秘密かぎ情報が格納されている。なお、カード有無を判定する方法として、第1利用者カード制御装置15、第2利用者カード制御装置16に付加されるカード検出センサの状態を確認する方法や、利用者カード6に対してISO7816に規定される条件で電源、クロック、リセットを供給して得られるATR (Answer To Reset) の情報から確認する方法等がある。

【0025】

利用者カード6の装着状態を検出すると(302)、利用者カード6に記憶さ

れている暗号化された販売元固有の秘密かぎ情報を取得するために、利用者ユニット制御手段が第1利用者カード制御装置を介して秘密かぎ情報の取得を行うためのコマンド情報を送信する。利用者カード6ではコマンド情報を受けた後、販売元固有の秘密かぎ情報をレスポンス情報として送信する。また、暗号化された販売元の秘密かぎ情報を復号化するために利用者カード固有の情報（第1利用者の秘密かぎ情報）を併せて送信する（303）。

【0026】

販売元固有の秘密かぎ情報と第1利用者固有の秘密かぎ情報をレスポンスとして受信した利用者ユニット制御手段は、暗号化情報再生器14に、販売元固有の秘密かぎ情報と第1利用者固有の秘密かぎ情報を送信して（304）、販売元固有の秘密かぎ情報を復号化させる（305）。ここで、暗号化情報再生器14では、規定の暗号形式で暗号化した際に利用した第1利用者固有の秘密かぎ情報を入力情報とし、逆関数による計算を行い、復号化した販売元固有の秘密かぎ情報を利用者ユニット制御手段22へ出力情報として返す（306）。販売元固有の秘密かぎ情報を受信した利用者ユニット制御手段22は、暗号化情報再生器14からレスポンスにより、再びデジタル情報格納媒体制御装置17に装着されているデジタル情報にアクセスして再生用情報部分のデータを取得する。この再生情報部分のデータは、暗号化されていて、このままでは利用できない。したがって、再生情報部分の復号化のためには、販売元固有の秘密かぎ情報が必要となる。そこで、先に取得した販売元固有の秘密かぎ情報と、この再生情報部分のデータを暗号化情報再生器14に送信して（307）、再生情報部分に付加されている暗号部分を解除した再生情報をレスポンスとして取得する（308）。

【0027】

続いて、この再生情報をデジタル情報再生手段20においてデータ変換処理やデータ圧縮状態を解凍する処理を行い（309）、その出力を利用者側入出力手段21へ入力することでデジタル情報の映像、音楽などの情報としての利用を可能とする（310）。なお、この復号化は、デジタル情報の再生する毎に行うものとする。ここで、利用者側入出力手段21はデジタル情報制御装置に内蔵されるもので、外部からのモニタリングは不可能な構成とする。例えば、無

理にデジタル情報再生手段20と利用者側入出力手段21の間の信号をモニタリングした場合、あらかじめ組み込んであるモニタリング防止機能が動作してデジタル情報再生手段20の動作を禁止する構成とする。なお、デジタル情報の再生処理において、利用者への操作の手順などを上記利用者側入出力手段21に表示したり、利用者が不正なICカードを利用した場合などのエラー処理を同じように利用者側入出力手段21の音声出力部により利用者に通知するようにしても良い。

【0028】

また、履歴情報として、デジタル情報の再生処理の各シーケンスをデジタル情報制御装置情報記憶手段18に格納する。履歴情報は、不正処理に対する追跡用情報や、故障、システムエラーなどが発生した場合のメンテナンス用情報として利用することができる。利用者側外部通信手段23を介して、デジタル情報制御装置1と外部機器とを接続することにより、オンラインによる通信が可能となる。利用者側外部通信手段23を利用し、故障、システムエラーの発生した場合の装置側の対策情報をオンライン経由で販売元の装置から送信すれば、リアルタイムの修復を行うことが可能となる。

【0029】

次に、図4を用いて、本実施例の特徴である、第一利用者から第二利用者（直接、販売元からデジタル情報の購入をしていない利用者）へのデジタル情報複写手順について、説明する。そして、図5を用いて、第1利用者所有及び第2利用者所有のICカード（以下第2利用者カードとする）の詳細な構成について説明する。

本実施例においては、キー情報の複写は、第1の記憶媒体に記憶された秘密かぎ情報プログラムに従って、図1のデジタル情報制御装置13が行う。また、デジタル情報2については、デジタルデータ格納媒体23から、不図示の第2の利用者のデジタルデータ格納媒体に複製させることとする。デジタルデータ2の複製は、いつ行ってもよいが、以下の販売者格納エリアに販売させた後や、販売元固有の秘密かぎ情報を第2の利用者のICカードに書きこんだ後が好ましい。

【0030】

まず、第1利用者カード制御装置及び第2利用者カード制御装置16に第1利用者と第2利用者のICカードをそれぞれ装着することにより、複写処理を開始する。両者のICカードが各利用者カード制御装置へ装着される(400)と、利用者ユニット制御手段は電源、クロック信号、リセット信号を第1利用者カードと第2利用者カードの入出力部30及び40へ供給する(401)。

【0031】

続いて、第1利用者カードから、デジタル情報の購入履歴と、デジタル情報を利用するための販売元固有の秘密かぎ情報を格納している履歴とを示す購入履歴情報をレスポンスとして返信する。この購入履歴情報は第1利用者カードに内蔵される履歴格納メモリ31から取得される。また、第1利用者カードから、購入履歴情報と併せてデジタル情報を購入するための価格情報を返信する。価格情報は、先のデジタル情報販売処理により第1利用者カード1に書き込まれた制御プログラム(秘密かぎ情報制御プログラム格納メモリ33に格納)に格納されている。これら2つの情報(購入履歴情報、価格情報)を利用者ユニット制御手段が受信する(402)と、金額徴収のシーケンスへ遷移する。

【0032】

続いて、第2利用者カードに対して、電子マネー情報を取得するためのコマンドを第2利用者カード制御装置16を介して第2利用者へ送信して、第2利用者カードよりICカード内の残金を示す残金情報をレスポンスとして取得する(403)。続いて、残金情報により価格情報を満足する残金が第2利用者カードにあると判定すると(404-YES)、第2利用者のICカード内の電子マネー格納メモリ46に、販売元が唯一アクセス可能な販売者専用エリア46-2を作成して(405)、価格情報に相当する電子マネー情報を販売者専用エリア46-2へ格納する(406)。結果として、第2利用者が使用できるエリア46-1から価格情報相当分の電子マネー情報を減額して、販売者専用エリア46-2へ価格情報相当分の電子マネー情報を増額することになる。ただし、この電子マネーの加減算については、単にデータの読み出しとその値に対する加減算を行うのとは異なり、第2利用者カードに記憶される電子マネー制御プログラム(電子

マネー制御プログラム格納メモリ47に格納される)によりプロトコル、通信データの暗号処理、また、第2利用者固有の情報を利用した認証処理を行いセキュリティ面で充実した処理を行う。

【0033】

続いて、第2利用者カードから第2利用者固有の暗号化情報を、第2利用者カードのロック管理メモリ45から取得して(407)、第2利用者固有の暗号化情報を第1利用者カードに送信する(408)。この後、第1利用者カード内部において、受信した第2利用者固有の暗号化情報をもとに、販売元固有の秘密かぎ情報の再暗号化処理を行う。手順としては、第1利用者のICカード内の販売者秘密かぎ暗号化情報エリア34-2に格納の暗号化された販売元固有の秘密かぎ情報と、第1利用者秘密かぎエリア34-1に格納の第1利用者秘密かぎ情報を、第1利用者カードの演算手段38が取得して、第2利用者より取得した第2利用者暗号化情報を併せて、暗号化又は復号化処理を行うための販売元固有の秘密かぎ情報を、暗号復号化処理手段32へ送信する(409)。次に、秘密かぎ情報暗号復号化処理手段32では第2利用者暗号化情報で販売元固有の秘密かぎを暗号化する。ここでは、第1利用者秘密かぎで販売者秘密かぎに施されている暗号化情報を解除した後、第2利用者暗号化情報により販売者秘密かぎを暗号化する。この結果として、第2利用者秘密かぎで復号可能な暗号化された販売者秘密かぎが生成される(410)。このように、秘密かぎ情報の暗号化と復号化処理をICカード内部で処理させることにより、外部からのモニタリングやデータの改ざんなどの不正アクセスに対するセキュリティを担保することができる。

【0034】

次に、第2の利用者暗号化情報に基づき暗号化された販売元固有の秘密かぎ情報をレスポンスとして、利用者ユニット制御手段が受信して、第2利用者内の暗号化された販売者秘密かぎを格納するためのエリア44-2へ、第2の利用者暗号化情報に基づき暗号化された販売元固有の秘密かぎ、を書き込む(411)。また、このとき、利用者間における販売元固有の秘密かぎ情報の複写の際の制御や、判愛社エリアの料金の回収を行う秘密かぎ情報制御プログラムを、第2の利用者カードに併せて書き込む。

【0035】

ステップ411の手続において、販売者秘密かぎが書き込まれたことを示す情報を、履歴格納メモリ41へ格納することにより、この情報を利用して不正な複写を取り締まる。また、複写の回数や販売元から数えて何回目の複写になるか等を書きこむこととすれば、世代管理が可能となる。販売元固有の秘密かぎ情報の複写処理を制御するプログラムに、世代管理を行うための情報を反映させて複写に関する限定を付加するようにしても良い。

【0036】

なお、複写処理を開始する際、必ず利用者に対して、“この情報の複写は有償です。”の旨を表示または通知することで、利用者の意思で複写処理が行われたことを確定する方式を採用するとよい。

【0037】

上記処理により第1利用者から第2利用者への第2の暗号化販売者秘密かぎの複写及び購入料金を、第2利用者のICカード内の販売者専用エリアへの格納ができたことになる。

【0038】

なお、上記説明では、「複写」処理について記述した。複写処理により、第1利用者と第2利用者の両方に販売元秘密かぎが存在することになる。しかし、第2の利用者に書くのエリアにのみ販売元秘密かぎが存在し、第1利用者の格納エリアには販売元秘密かぎが秘密かぎが存在しない秘密かぎの「移動」処理を行わせてもよい。移動処理を行うためには、第2利用者への秘密かぎ情報の書き込み完了時点で、第1利用者カード内の販売者秘密かぎ格納エリア34-1に格納される、第2の暗号化販売元秘密かぎ情報を消去すればよい。つまり、複写処理は、秘密かぎが増加する処理であり、個人間の転々流通を利用して販売の拡大を目的とする場合に有効な方法である。一方、移動処理は、秘密かぎが移動処理によっては増加せず、販売字にその総数が決まる“限定発売”の形態でデジタル情報を配信するような場合に有効な方法である。

【0039】

本実施例によれば、履歴を記録することとしたため、販売元から利用者への直接

的に販売した絶対数を管理することが可能となる。市場に提供する利用可能なデジタル情報の総数管理を販売元により一元化する場合に有効である。

【 0 0 4 0 】

なお、本実施例においては、販売元固有の秘密かぎ情報を、それぞれ第 1 の利用者固有の秘密かぎ情報や、第 2 の利用者固有の秘密かぎ情報で暗号化する、高度なセキュリティを持つ例を説明した。しかし、これに限らず、販売元固有の秘密かぎ情報を利用者固有の秘密かぎ情報で暗号化しなくても、本実施例の効果を有するものとなる。

【 0 0 4 1 】

また、本実施例においては、デジタルデータ 2 を利用者のデジタルデータ格納媒体 2 3 に記憶させる構成としたが、利用者カード 6 に秘密かぎ情報と共にデジタルデータ 2 を記憶させてもよい。

【 0 0 4 2 】

また、利用者カード 6 に、販売元固有の秘密かぎ情報を記憶させることとしたが、デジタルデータ格納媒体 2 3 に、デジタルデータ 2 と共に、販売元固有の秘密かぎ情報を記憶させてもよい。

【 0 0 4 3 】

なお、本実施例において、販売元固有の秘密かぎ情報の複製の際に、販売者エリアへ販売金額を格納させることを説明した。このような制御は秘密かぎ情報制御プログラムに規定されている。秘密かぎ情報制御プログラムは、デジタル情報販売装置 1 がデジタル情報の販売と共に利用者カードに書きこまれる。なお、上述のように、秘密かぎ情報制御プログラムをデジタルデータと共に、デジタルデータ格納媒体に記憶させてもよい。秘密かぎ情報制御プログラムは、当然、販売元固有の秘密かぎ情報の複製時に第 2 の利用者のカードや媒体に記憶される。また、秘密かぎ情報制御プログラムをデジタルデータの複製時に複製させるのではなく、販売元固有の秘密かぎ情報の複製時に販売者エリアへ販売金額を格納させる制御機能を、デジタルデータ制御装置 1 3 に予め持たせておいてもよい。次に、図 6、図 7 を用いて、販売者エリア 4 6 - 2 に格納された販売金額（電子マネー情報）を回収する方法を説明する。あわせて、第 2、第 3 ・ ・

第n利用者間の購入金額に相当する電子マネー情報の移動方法を説明する。

まず、図6において、販売店50はデジタル情報の販売元である。デジタル情報51は暗号化が施されていないデジタル情報である。販売元固有の暗号化情報52は、販売するデジタル情報51を販売元固有の暗号化情報で暗号化する。販売元固有の秘密かぎ情報53は、データの復号化の際に利用ものである。販売元が所有するICカード54は、利用者から購入料金（電子マネー）を格納することなどに利用する。デジタル情報55は販売元の暗号化情報52で暗号化された情報である。利用者については、第1、第2、第3、第N利用者について記述する。第1利用者60は、販売元からデジタル情報55を購入する。第1利用者固有の秘密かぎ情報61は、同利用者の暗号化情報であり、同利用者所有のICカード63には、電子マネー情報が少なくとも格納されているものとする。情報64は販売元固有の秘密かぎ情報を第1利用者固有の暗号化情報で暗号化されたものであり、この情報を購入する場合、第1利用者は第1利用者固有の暗号化情報を販売元に渡すことでこの情報が作成される。なお、第2、第3利用者及び第N利用者に対する構成は第1利用者と同様な構成となっている。ただし、販売元固有の秘密かぎ情報74は第2利用者固有の暗号化情報により第1利用者カード内で暗号化された情報であり、販売元固有の秘密かぎ情報84は第3利用者固有の暗号化情報により第2利用者カード内で暗号化された情報であり、販売元固有の秘密かぎ情報94は第N利用者固有の暗号化情報により第N-1利用者カード内で暗号化された情報である。

【0044】

販売元と第1利用者間の販売手順及び第1利用者と第2利用者との複写処理については、先に説明した手順により行うものとして、ここからは第2利用者から第3利用者及び第N利用者までの複写処理とその際に発生する料金の遷移状態について説明する。

第2利用者から第3利用者へのデジタル情報55の複写に伴い、第3利用者はこの情報を利用するために、販売元固有の秘密かぎ情報が必要となる。この場合、デジタル情報55自体は販売元固有の暗号化情報で暗号化されているので複写をすることにはなんら問題はない。また、暗号化された販売元固有の秘密か

ぎ情報を複写しても暗号化されていて、販売元により許可された利用者以外がこの情報を取得しても利用できないので、これもまた問題はない。

【0045】

さて、第3利用者固有のICカードに第2利用者と同様に販売元固有の秘密かぎ情報74を複写することがデジタル情報を販売元から購入したということになり、第一利用者と同様に購入料金の支払が発生する。先の例によれば、第2利用者においても第1利用者から上記秘密かぎ情報74を購入した際、購入料金に相当する電子マネー情報が徴収されていることになっている。

【0046】

そこで、図7を用いて、第3利用者カードについて、カード内に格納されている電子マネー情報の販売元との関係を説明する。まず、第3利用者から料金（ここでは購入料金を¥100とする）を徴収する（701）。この購入料金は電子マネー情報の移動により成立する。実際には第3利用者が所有するICカード83の電子マネー情報格納メモリに販売元専用エリアを作成して、この販売元専用エリアに購入料金に相当する電子マネー情報を移動させる。これは、図5を用いて説明したものと同様な構成とする。また、料金徴収の例を述べると、第3利用者のICカード83に¥500格納されていて、料金¥100がこのエリアから引き出されて、新しく作成した販売元専用エリアに¥100が追加格納される。この時、電子マネー情報の増減については結果として各エリアの電子マネー情報に対して加減算が行われたようになるが、実際は暗号化データに対する計算処理を行い、高いセキュリティに保護されて実行されているものである。

【0047】

購入料金が徴収完了する（702-yes）と、次に第3利用者の暗号化情報82を取得する（703）。そして、第3利用者の暗号化情報82と第2利用者の秘密かぎ情報71及び第2利用者の暗号化情報72で暗号化された販売元固有の秘密かぎ情報74との3つの情報により第3利用者の暗号化情報82で暗号化された販売元固有の秘密かぎ情報84を作成する（704）。次に、第3利用者の暗号化情報で暗号化された販売元固有の秘密かぎ情報84を第3利用者のICカードへ書き込む（705）。この情報の書き込みが完了することで第3利用者

はデジタル情報 55 を利用できることになる。以上の動作は、図 4 で示した第 2 の利用者への複写と同様である。

【 0 0 4 8 】

ここで、デジタル情報購入料金について考えてみると、第 3 利用者への複写処理が半ば完了した時点で、第 2 利用者及び又は第 3 利用者の各々の IC カードに販売元専用の電子マネー情報が格納されていることになる。この販売元が回収すべき購入料金（電子マネー情報）を効率良く回収するために、後続の利用者が希望する複写（販売元固有の秘密かぎ情報の複写）とリンクさせて、後続の利用者のカード内に電子マネー情報を移動させる。

【 0 0 4 9 】

つまり、第 3 利用者の複写元となる第 2 利用者に販売元専用電子マネー格納エリアが存在することになる。そして、対象となるエリアの電子マネー情報の格納状態を確認する（706）。第 2 利用者の IC カードに購入料金がある（706 - y e s）場合は、第 2 利用者の IC カードから対象となる電子マネー（購入料金相当）を第 3 利用者の IC カードへ格納する（707）。ここでの電子マネー情報の移動に関しては、先に第 3 利用者の IC カード内に格納した販売元専用のエリアへ電子マネー情報をセキュリティに保護されて格納することになり、結果として、第 3 利用者の販売元専用の電子マネー格納エリアの電子マネー情報が加算されたことになる。以降第 3 利用者から第 4 利用者の複写処理及び後続の利用者間の複写処理についても第 2 利用者から第 3 利用者への上記購入料金が移動と同様の手順で行われる。最後にデジタル情報とその利用に必要な販売元固有の秘密かぎ情報の複写に関して、第 $n - 1$ 利用者と第 n 利用者（最終複写先となる利用者）間の複写処理が終了する（708 - n o）と上記手順で第 n 利用者の IC カードの販売者専用エリアに格納された購入料金 x は、下記に示す式で計算することができる。

【 0 0 5 0 】

$$x = \text{デジタル情報の購入料金} \times (n - 1) \quad (\text{ただし } 2 \leq n)$$

本実施例において、最終複写先を第 8 利用者とし、また、デジタル情報の購入料金を一律 100 円と仮定すると上記手順により第 8 利用者への複写処理が完了

時点で、販売元が徴収可能な電子マネーは総額 7 0 0 円となり、これが第 8 利用者の IC カードに格納されている。

【 0 0 5 1 】

第 8 利用者から販売元が蓄積された購入料金を回収する方法として、第 8 利用者のデジタルデータ制御装置がオンラインの環境下で稼動する場合、第 8 利用者が対象となるデジタル情報を利用する時点で、第 8 利用者カードに記憶されている購入料金回収プログラム（第 7 利用者から第 8 利用者や販売元固有の秘密かぎ情報の複写の際、同様に第 8 利用者カードへ書き込まれているもととする。）により格納されているすべての料金をオンラインで販売元所有の IC カード 5 4 へ移動させることで回収できる（ 7 0 9 ）。

【 0 0 5 2 】

また、第 8 利用者のデジタル情報制御装置がオフラインの環境下で稼動する場合、購入料金回収プログラムにより第 8 利用者に対して、販売店へ IC カードを持参すると蓄積された料金に対応して返金サービスが受けられるなどの情報を通知することで蓄積された購入料金の回収経路を確保することができる。また、返金サービスの他にも最新の情報を IC カードを利用して提供するなどのサービスを行うことで、より一層高い回収率が望めることになる。また、秘密かぎ情報はデジタル情報個々に異なるものなので、複数のデジタル情報を利用する場合、各秘密かぎ情報に対して販売元専用の電子マネー情報格納領域へ個別に格納すると購入料金回収時の処理に対して利便性が向上する。また、販売元固有の秘密かぎ情報の格納メモリの制約により、複写のためのメモリ容量が不足する場合には、その旨を利用者に通知するようにしても良い。なお、本実施例においては、第 8 利用者がオンラインにより販売元エリアの金額を送付することを説明したが、第 2 利用者がこれを行ってもよいことはいうまでもない。

【 0 0 5 3 】

上記の実施例においては、販売元固有の秘密かぎ情報と購入料金に相当する電子マネー情報がリンクして移動する場合について説明した。次に、利用者の動作環境を示す情報と販売元との過去の取引履歴を示す情報を利用することで、オフラインの環境下に蓄積される購入料金の移動を更に効率良く回収する方法につい

て、図 8、図 9 及び図 1 0 を用いて説明する。

図 8 は販売元及び販売元からデジタル情報を購入した第 1 利用者から第 n 利用者までのデジタル情報制御装置の環境を示したものである。デジタル情報販売装置 1 0 0 は回線に接続され外部との通信機能を少なくとも備えるデジタル情報販売装置 1 であり、販売元が管理するものである。デジタル制御装置 1 0 1、1 0 4、1 0 8、1 0 9 は利用者が所有する装置であり、これには回線に接続され外部との通信機能を少なくとも備えるものとする。また、デジタル情報制御装置 1 0 2、1 0 3、1 0 5、1 0 6、1 0 7 は利用者が所有する装置であり、これには回線に接続され外部との通信機能はないものとする。また、デジタル情報販売装置 1 0 0 を含め、1 0 1 から 1 0 9 までの各装置を所有する利用者及び販売者は IC カードを所有していて、その中には電子マネー情報、購入履歴情報などが格納されているものとする。ただし、購入履歴に関する情報は販売元と直接的な取引が行われた場合に記憶されるものとする。1 1 0 は、各装置が接続する回線であり、電話回線、専用回線などである。

【 0 0 5 4 】

まず、第 1 利用者と販売元におけるデジタル情報の販売において、先の実施例で説明した方法により販売元固有の秘密かぎ情報を、第 1 利用者の IC カードに書き込む際、購入時刻や販売元の利用回数を示す情報を第 1 利用者の IC カードの履歴格納エリアに、一緒に書き込む。ここで書き込む内容について図 9 を用いて説明する。

【 0 0 5 5 】

なお、ここでは第 1 利用者カードの内容を例にして説明する。デジタル情報の購入した日付情報を格納するための購入日格納エリア 1 2 5 - 1 に購入日に関する情報として、年月日、時刻を書き込む。この情報は販売元との最新取引を管理するものとして取り扱うため、販売者と利用者間の取引では必ず記録を行うこととする。ただし、元の購入日を新しい情報に更新する形式としても良いし、新しい購入日を追加する形式としても問題ない。また、上記購入日の書き込みと同様に販売元の利用回数を示す情報を書き込むための利用回数エリア 1 2 5 - 2 に販売元と第 1 利用社の取引が行われる毎に利用回数を更新（カウントアップ）す

る。なお、販売元との取引については、第1利用者のようにオンライン環境下で稼動可能な端末の場合、デジタル情報の配信と購入料金決済（電子マネー情報による）及び販売元固有の秘密かぎ情報の書き込みをオンラインでリアルタイムに実行しても良い。また、販売元（販売店など）まで出向いて、そこで上記情報の書き込み処理を含む取引を行っても良い。販売元と利用者間の取引については、確実に購入料金を回収可能であるが、この後、第1利用者以降第n利用者までの購入料金をいかに回収するかが問題となる。そこで、第1利用者から第2利用者への複写処理で徴収される購入料金の遷移の仕方を基本として、以降第n利用者までの購入料金の遷移をICカードに格納される購入来歴情報により制御する方法について説明する。

【0056】

第1、第2利用者間で販売元固有の秘密かぎ情報を複写するための複写処理は、第1利用者又は第2利用者の環境下で行う。すなわち、第2利用者のICカードに格納され、かつ、第2利用者専用エリアに格納される電子マネー情報から販売元専用エリアに購入料金相当の電子マネー情報を格納して、次に、第1利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報を第2利用者固有の暗号化情報により暗号化された販売元固有の秘密かぎ情報という形式にするため暗号化及び復号化処理を行う。そして、この情報を第2利用者のICカードに書き込む。一連の処理を行った後、第1利用者及び第2利用者のICカードから購入来歴情報を取得する（1000）。この処理で取得可能な情報として、購入日格納エリア125-1に格納される購入日情報と利用回数エリア125-2に格納される利用回数情報の2つであり、第1、第2利用者に対するこの2つの情報を比較して、電子マネー情報を移動させることになる。ここでは、比較条件を購入日情報に限定し、かつ、両者の購入日情報により古い日付から新しい日付のICカードの方向へ上記購入料金を移動させることにする。1000で取得した購入日情報を西暦により取扱い全部で7バイトのデータで定義する（年を示す値に2バイト、月を示す値に1バイト、日を示す値に1バイト、時間を示す値に1バイト、分を示す値に1バイト、秒を示す値に1バイトを割り当てる）と第1利用者の購入日が1999年03月01日13時00分00秒の場合（1001-y

e s)、

H '136303010D0000 (16進数表記)

として取り扱う。また、販売元との直接的な取引がない場合 (1001-no)、そのICカードには購入日情報がないので、

H' FFFFFFFF FFFFFFFF (16進数表記)

として値を代用する (1002)。この条件により、第 $n-1$ 利用者の購入日情報を $X1$ 、第 n 利用者の購入日情報を $X2$ とすると、 $X1 \leq X2$ の場合、両者のICカードに格納される購入料金の全額を第 $n-1$ 利用者のICカードへ格納する。図8の例では第1利用者には購入日情報 (1999年3月1日) があり、第2利用者には購入日情報がないので、この場合、第1利用者のICカードに購入料金が格納される。上記の方法で第2利用者以降第 n 利用者までの利用者間の複写処理を繰り返し行う (1006-yes)。最後の第 n 利用者と第 $n-1$ 利用者間の複写処理が終了する (1006-no) と結果として購入日情報が格納されているICカードへ購入料金が格納されていくことになる。また、購入日情報の代わりに利用回数情報の順位を優先して、利用回数の多い方向へ移動させることにしても良い。ただし、この場合、販売者と直接取引がない場合の利用回数情報をH '00 (16進数表記) で取扱い、第1利用者の利用回数情報を $Y1$ 、第2利用者の利用回数情報を $Y2$ とすると、 $Y1 \geq Y2$ の場合、両者のICカードに格納される購入料金の全額を第1利用者のICカードへ格納する。このように販売元との直接的な取引があり、かつ、その取引が最近に確立された又は利用頻度の多いICカードへ購入料金を移動させることで、販売元への回収率がより一層向上する。

【0057】

更に購入料金の回収状況を向上させる方法として、図9のプロバイダ契約情報格納メモリに格納される情報により購入料金の移動を制御する方法が考えられる。すなわち、第1利用者から始まる利用者間の複写処理のリングの中でオンライン環境下で稼動する装置の利点を活用して、オフライン環境下で稼動する装置を所有する利用者間で蓄積された購入料金を一括して販売元に送信 (回収させる) する方法である。この方法は上記で説明した購入日情報及び利用回数と組み合わせ

せて実施しても良いし、プロバイダ契約情報格納メモリ 1 2 4 に格納される情報に特化して実施しても良い。ここでは組合せによる実施例について下記に述べるが、前提条件として、利用者がインターネットなどのネットワーク上に配信される情報を利用者する環境の情報として、ネットワークにアクセスするためのサーバを提供する会社名やその連絡先を示す電話番号又はサーバ固有の番号などを格納するためのプロバイダ契約情報格納メモリ 1 2 4 にあらかじめ各種情報（以下プロバイダ情報）を格納してあるものとする。また、第 n 利用者の IC カードに格納され、かつ第 n 利用者専用エリアに格納される電子マネー情報から販売元専用エリアに購入料金相当の電子マネー情報を格納した後、第 $n - 1$ 利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報を第 n 利用者固有の暗号化情報により暗号化された販売元固有の秘密かぎ情報という形式にするため暗号化及び復号化処理を行い、この情報を第 n 利用者の IC カードに書き込むまでの一連の処理を行った後の処理について説明する。

【 0 0 5 8 】

まず、第 $n - 1$ 利用者のプロバイダ契約情報格納エリアの情報を取得して、プロバイダ情報があれば (1 1 0 0 - y e s)、第 $n - 1$ 利用者の IC カードに両者の IC カードに格納される購入料金をすべて格納する (1 1 0 1)。もしも、第 $n - 1$ 利用者の IC カードにプロバイダ情報が無い場合 (1 1 0 0 - n o)、第 n 利用者のプロバイダ契約情報格納エリアの情報を取得して、プロバイダ情報があれば (1 1 0 2 - y e s)、第 n 利用者カードに両者の IC カードに格納される購入料金をすべて格納する (1 1 0 3)。もしも、第 n 利用者の IC カードにプロバイダ情報が無い場合 (1 1 0 2 - n o)、両者の購入日情報を取得した (1 1 0 4) 後、この情報を比較する。第 $n - 1$ 利用者の購入日情報を $X 1$ 、第 n 利用者の購入日情報を $X 2$ として、 $X 1 < X 2$ の場合 (1 1 0 5 - y e s)、第 n 利用者側に格納する (1 1 0 6)。なお、 X は日付が新しいほうが大きい数をもつものとする。 $X 1 > X 2$ の場合 (1 1 0 7 - y e s)、第 $n - 1$ 利用者側に格納する (1 1 0 8)。また、 $X 1 = X 2$ の場合、両者の利用回数情報を取得した (1 1 0 9) 後、この情報を比較する。第 $n - 1$ 利用者の利用回数情報を $Y 1$ 、第 n 利用者の利用回数情報を $Y 2$ として、 $Y 1 < Y 2$ の場合 (1 1 1 0)、

第 n 利用者側に格納する (1 1 1 1)。上記以外の場合、第 $n - 1$ 利用者側に格納する (1 1 1 2)。この手続きを続ける場合 (1 1 1 3) は、 N に 1 を加え、ステップ 1 1 0 0 に戻る。また、購入日情報及び利用回数情報が書き込まれていない場合については、先に説明した手順で値を代入して比較することになる。

【 0 0 5 9 】

上記の手順で格納された購入料金の移動方向は、第 1 にプロバイダ情報がある IC カードに格納され、第 2 に複写した日に 1 番近い日に販売元と取引を行った履歴のある IC カードに格納され、第 3 に利用回数が多く、販売元との取引確率の多い IC カードに格納されることになる。上記の購入料金が格納された IC カードで、特に、プロバイダ情報が格納されている IC カードから購入料金を回収するタイミングは利用者がインターネットなどのネットワークにアクセスする際、あらかじめ記憶してある販売元の連絡先を示す電話番号に回線経由で自動的にダイヤリングしてアクセスを行い、回線経由で利用者の IC カードから購入料金に相当する電子マネー情報を全額を送信して、販売元の IC カードの電子マネー格納エリアに格納することで回収を完了する。この回線経由の通話料金については、販売元が負担するためフリーダイヤルなどを設定することで利用者に負担がかからないようにする。この方法によれば、オフライン環境下に埋もれてしまいがちな販売元が回収できる電子マネー情報を効率良く、かつ、高確率で回収できるようになる。

【 0 0 6 0 】

次に、利用者の IC カードなどに記憶媒体に複数のアプリケーションが格納されており、デジタル情報の購入に直接関与しないアプリケーションを利用してデジタル情報の購入料金を回収する方法について説明する。

図 1 2 は本実施例のシステムを示す構成図であり、デジタル映像販売元 1 4 0 はデジタル映像などのデジタル情報を販売する。銀行 ATM 1 4 1 は銀行における引き出し、預け入れ、振り込みなどの処理が可能である。金額情報格納メモリ 1 4 2 は利用者の金額情報を格納する。利用者専用エリア 1 4 2 - 1 は利用者 1 が使用できる電子マネー情報を格納する。販売者専用エリア 1 4 2 - 2 は利用者 1 の IC カードにある販売元が購入料金を回収するためのエリアである。

銀行ATM用AP143は利用者1のICカード130にあり、電子マネーによる決済用AP、ポイント管理用APなどが格納されているAPメモリである。キー管理メモリ144はデジタル映像を再生するために必要なキー情報144-1が格納されている。また、第2の利用者カード131は、第1の利用者のICカード130と同等の構成とする。

【0061】

まず、デジタル映像販売元140から利用者1は情報に対する支払を済ませると利用者1のICカード132にあるキー管理格納エリア144へデジタル映像145を再生するためのキー情報144-1とデジタル映像145を書き込んでもらう。ここでデジタル映像はICカードに格納せず、ICカードと異なる別の記憶媒体に格納しても良い。ここでは、ICカード内に格納することにする。利用者1ICカードに格納されたデジタル映像145及びキー管理エリアに格納されたキー情報144-1により利用者1はデジタル映像145を生成することが可能になったことになる。次に、この利用者1から利用者2へキー情報144-1をコピーする際の手順では、利用者2の利用者専用エリア147-1からデジタル映像の購入料金（この場合300円）の電子マネー情報を販売元専用エリア147-2へ格納することでキー情報のコピーを許可する。ただし、この制御は利用者2のAPメモリ146に格納されている電子決済用APにより行われるもので、この電子マネーAPはキー情報144-1のコピー開始時に利用者1から利用者2へコピーされたものである。また、利用者1は販売元との決済時に利用者1のAPメモリ143に販売元よりコピーされたものである。購入料金として販売者エリアに電子マネーが格納されたことにより、キー情報のキー管理エリアへのコピーが許可されて、利用者2はデジタル映像145を再生可能な状態になる。ここでポイントとなるのは、キー情報のコピーに必ず販売元エリア147-2への電子マネー情報の格納動作が付随していることにある。

【0062】

利用者エリア147-1における残金が不足している場合、このキー情報のコピーは禁止して、デジタル映像145の再生を不可能にする。また、販売元専

用エリア147-2に格納された電子マネー情報は常に販売元固有の情報によりロック状態となっており、利用者2が利用しようとしても不可能である。このロック状態を解除するためには販売元固有の情報を入力することが必要である。このように電子マネー情報の格納処理やロック状態の制御などは電子決済用APにすべて準じて行われる。これらの動作は上述の実施例と同様である。

【0063】

次に、利用者2の販売元専用エリア147-2に購入料金として格納された電子マネー情報の回収について図13の手順を示すフローチャートにより説明する。利用者2のAPメモリには銀行ATM用APが格納されていて、利用者2は銀行にて、このICカード135を使って預金や引き出し及び振り込みなどが行えるものとする。ここで、利用者2が銀行ATM141により振り込みを行うと、APメモリに格納される銀行ATM用APが起動する(1300)。この起動に関しては、ここでは図示せぬアプリケーション管理APが電子決済用APへ購入金額の格納の有無を確認した後、銀行ATM用APを起動することにする。ここで、販売元専用エリア147-2に購入料金が格納されていると上記の確認で判明した場合(1301-yes)、電子決済APにより銀行ATM141へ購入料金の全額を送金する(1302)。銀行ATM141は購入料金を受け取ると、続いて購入料金を送金する販売元の連絡先を示す情報を利用者2ICカード135より受け取る。この連絡先を示す情報も電子決済用APが制御して送信する。購入金額と販売元の連絡先情報を受け取った銀行ATMは即座に販売元と回線接続をして(1303)、利用者2から受け取った購入金額をすべて販売元140に送金する(1304)。送金が完了すると販売元140と銀行ATM141間の回線接続を切断して(1305)、銀行ATMのサービスを実行する。このタイミングで利用者2のICカード内でも電子決済APから銀行ATM用APに切り替わり、振り込み処理が可能になる。利用者2の振り込み処理の終了時点では、既に販売元140への回収が完了したことになる。

【0064】

本実施例によれば、1枚のICカードで複数のアプリケーションを利用できる構成として、デジタル情報の再生以外(例えば、ショッピングや銀行振り込み

など) で I C カードを利用する際、バックグラウンド処理により I C カードに蓄積された料金を販売元に振り込む方式を採用することで、利用者の意図する行動を利用した販売元と利用者間の料金回収ルートの拡張が可能である。

【 0 0 6 5 】

上記の実施例では、利用者の意図する振り込み処理の前に購入料金を販売元までの銀行 A T M を経由してデジタルデータ販売元へ送金処理を行っているが、これを銀行 A T M で一次保管して、利用者と銀行 A T M 間の振り込み処理の終了時に改めて販売元へ送金するような形式の実施例について、その手順を図 1 4 に示して説明する。

デジタル映像 1 4 5 の購入料金を販売元専用エリア 1 4 7 - 2 へ格納してある状態で利用者 2 が銀行 A T M を利用する場合、利用者 2 は I C カード 1 3 5 を銀行 A T M 1 4 1 に装着して振り込み処理を実行することになる。この時、アプリケーション管理 A P と銀行 A T M 用 A P 及び電子決済用 A P の起動に関する関係は上記の例で説明したものと同様の動作となる。まず、銀行 A T M 用 A P が起動されるが (1 4 0 0) 、電子決済用 A P により販売元専用エリア 1 4 7 - 2 の格納状況を確認して (1 4 0 1) 、購入金額が格納されている場合 (1 4 0 1 - y e s) 、銀行 A T M 1 4 1 へすべての購入金額の送金と販売元の連絡先情報を送信して電子決済用 A P の処理を終了する (1 4 0 2) 。次に、利用者 2 の銀行 A T M 用 A P と銀行 A T M 間において振り込み処理を開始して (1 4 0 3) 、無事に振り込み処理を終了する (1 4 0 4) と利用者 2 の I C カードを排出する。ここで、カード排出の時点では既に購入料金は銀行 A T M へ送金されており、販売元への送金にはこの I C カードが A T M に装着されている必要はない。続いて、銀行 A T M は先に受け取った購入料金を確認して、販売元への送金がある場合 (1 4 0 5 - y e s) 、販売元へ送金するために回線接続を行う (1 4 0 6) 、回線の接続を正常に完了すると電子マネーによる送金を開始する (1 4 0 7) 、送金を正常に終了した後、販売元 1 4 0 と銀行 A T M 1 4 1 間の回線接続を切断して販売元への購入料金の回収を完了する (1 4 0 8) 。上記において、回線接続に失敗した場合などは再度接続するようにしたり、回収のための電子マネー情報の送金時にエラーが発生した場合の再送金処理の実行を行うとより一層の信頼

性が得られるようになる。

【0066】

上記例では、銀行ATMを利用して販売元へ利用者2の購入料金を送金することにしたが、買物の際に使用するクレジット用APで回収させるようにアプリケーション管理APを設定するようにしても良い。この場合、クレジット会社から販売元へ購入料金に対応する電子マネー情報を送金する形式やクレジット会社より販売元の銀行口座へ料金を振り込む形式が考えられる。また、上記例に対して、銀行ATM用APと電子決済用APの処理を並行して処理させ、利用者の振り込み処理のバックグラウンドで電子決済用APによる販売元への振り込み処理を実行するようにするとなお良い。このようにデジタル映像の再生アプリケーションと異なる別のアプリケーションを使って回収することで、販売元と利用者間の回収ルートが拡張され、販売元への回収のための処理を利用者に意識させずに、より確実に拡張性のある料金回収ルートが確立できる。

【0067】

以上の実施例における秘密かぎ情報の複製の制御や秘密かぎ情報の複写と共に販売エリアへの金額移動させる制御、販売エリアからセンターへ回収させる制御は、販売元等から配信、提供された秘密かぎ情報制御プログラムに規定されており、この秘密かぎ情報制御プログラムは、秘密かぎ情報の複製と共に、それぞれの利用者カードや、記憶媒体等に記憶される。

【0068】

本発明の第2の実施例を図15、図16を用いて説明する。本実施例は、デジタル情報とキー情報を複製する際には、キー情報を使用不可の状態に複製させ、センターへアクセスすることにより、キー情報を解除するものである。

図15に、本実施例のシステム構成を示す。デジタル情報販売元150はデジタル情報を販売するセンター等である。デジタル情報販売元150には、デジタル情報と、キー情報と、キー情報制御プログラムを含む販売者側プログラムを格納する記憶媒体を有するデジタルデータ販売装置が設置されている。サポートセンタ151はデジタル情報の利用に関する操作の説明、最新情報の紹介などを行う。

記憶媒体 1 5 3 は、第 1 の利用者の記憶媒体であり、記憶媒体はハードディスク、光磁気ディスク、磁気ディスク、ICカード、メモリーカード、SIMカードなど形態はなんでも良い。記憶媒体 1 5 3 は、販売元より購入したデジタル情報 1 5 4 を記憶する。デジタル情報 1 5 4 は、不正使用を防止するため、暗号化されている。メモリ 1 5 5 は、第 1 の利用者のデジタル情報利用のために必要な情報を格納し、デジタル情報 1 5 4 を使用するためのキー情報 1 5 6 を格納する。例えば、キー情報 1 5 6 は、暗号化されたデジタル情報 1 5 4 を複号化するための秘密かぎ等である。

記憶媒体 1 5 7 は、第 2 の利用者の記憶媒体である。記憶媒体 1 5 7 は、第 1 の利用者の記憶媒体 1 5 3 から複製したデジタル情報 1 5 8 を記憶する。メモリ 1 5 9 は、第 2 の利用者のデジタル情報利用のために必要な情報を格納する。キー情報 1 6 0 は、ロック情報 1 6 1 によりロック、つまり使用不可の状態にされる。

【 0 0 6 9 】

この構成において、デジタル情報 1 5 4 はキー情報 1 5 6 により利用可能となっている。まず、第 1 の利用者は、デジタル情報販売元 1 5 0 から、デジタル情報 1 5 4 とキー情報 1 5 6 に対する料金を支払うことにより、第 1 の利用者の記憶媒体 1 5 3 にデジタル情報 1 5 4 とキー情報 1 5 6 及びキー情報制御プログラムを書き込んでもらう。そして、第 1 の利用者は、デジタル情報 1 5 4 を再生する際に、キー情報 1 5 6 を用いて暗号化されたデジタル情報を複号化し、デジタル情報を再生する構成とする。なお、この複号化は、デジタル情報の再生する毎に行うものとする。以上の動作は、第 1 の実施例において説明したものと同様であり、図 1 おいて説明したデジタル情報販売装置 1 及びデジタル情報制御装置 1 3 を使用する。

【 0 0 7 0 】

次に、デジタル情報販売元 1 から情報を取得した第 1 の利用者から、第 2 の利用者へのデジタル情報を複写させる際の方法について説明する。

第 1 の利用者の記憶媒体 1 5 3 から、第 2 の利用者への記憶媒体 1 5 7 のデジタルデータ、キー情報の複製の際には、第 1 の実施例において説明した、ディ

ジタル情報制御装置 1 3 を使用する。ここで第 1 の実施例と異なるのは、キー情報の複製方法である。第 1 の実施例においては、キー情報を使用可能な状態にして、第 2 の利用者へ複写することとしたが、本実施例においては、第 2 の利用者へキー情報を複写する場合は、キー情報を使用不可の状態、ロック状態で複写する。なお、デジタル情報 1 3 4 のコピーについては上記で説明した通り、キー情報 1 3 7 が利用者の記憶媒体と一緒に存在しないと利用ができないので無制限に複写しても問題がない。また、第 1 の利用者カード 1 5 3 においては、キー情報 1 5 6 は、販売元から書き込まれた際、キー情報 1 3 7 の状態を示す情報はロック解除状態になっている。キー情報がロック解除状態であるため、第 1 の利用者は、デジタル情報 1 5 4 を再生できる。

【 0 0 7 1 】

第 1 の利用者から第 2 の利用者への複写の手順は以下の通りである。まず、第 1 の利用者から第 2 の利用者へデジタル情報の複写の指示を行う。指示が行われると、利用カード制御装置 1 5、利用者カード制御装置 1 6 を用いて、デジタル情報 1 5 4 と共に、キー情報の複製を行う。このとき、販売元から第 1 の利用者の記憶媒体に記憶されていたキー情報制御プログラムが、キー情報の複製を制御する。

【 0 0 7 2 】

第 1 の利用者から第 2 の利用者へのキー情報 1 5 6 の複製の際に、第 1 の利用者側でロック解除の状態であったキー情報 1 5 6 を、ロック状態にして、コピー先の第 2 の利用者の記憶媒体 1 5 7 に書き込む。

【 0 0 7 3 】

ここで、キー情報のロックについて簡単に説明する。キー情報は、1 Byte のヘッダー、データサイズを示す 1 Byte のデータ長、最大 2 4 9 Byte の商品名と 4 Byte の商品コードと 1 Byte のキー情報のロック状態を示すデータからなる最大 2 5 4 Byte のデータ、そして、ヘキサコード 1 Byte のチェックサムにより構成されるデータである。そして、複写元となる第 1 利用者の記憶媒体（カード内）に存在するキー情報制御プログラムは上記構成をなすキー情報に対して上記“ロック状態を示すデータ 1 Byte”の値を変更したキー情報を第 2 利用者の記憶媒体へ複写

するために生成する。例えば上記ロック状態を示すデータがロック解除の状態を意味する0の値となっている場合、この値をロック状態であることを意味する1の値に設定したキー情報を生成する。また、ロック状態の種別としては“ロック”、“ロック解除”の2つの状態の他にデジタル情報を10%利用可能であるロック状態を意味する2の値としたり、80%の利用が可能であるロック状態を意味する3の値としたりすることで、“ロックの状態”に複数の利用範囲を規定することも可能である。上記ロック状態に設定されたキー情報はデジタル情報制御装置の利用者ユニット制御手段22が利用者カード制御装置1(15)を制御して第一利用者の記憶媒体(ICカード内臓メモリ)より取得する。

【0074】

続いて第2利用者の記憶媒体に上記ロック状態に設定されたキー情報を複写(書き込み)するのはデジタル情報制御装置の利用者ユニット制御手段22が利用者カード制御装置2(16)を制御して第2利用者の記憶媒体(ICカード内臓のメモリ)へ上記キー情報を複写(書き込む)する。第1利用者記憶媒体及び第2利用者記憶媒体と利用者ユニット制御手段1及び利用者制御ユニット2との関係(装着、はめ込む)はどちらであってもよい。上記のようなロック状態を示すデータの変更を施したキー情報の生成はICカード内部で行うことで高い安全性を得られる。また、キー情報に対して上記キー情報管理プログラムで暗号化処理を施すことでより一層の安全性が得られる。

【0075】

なお、キー情報の記憶媒体への書き込みには必ず販売元固有のコードを利用し、このコードを利用しないで書き込みを行うと、キー情報137にロック情報138が必ず付加された形態で記憶媒体に書き込まれる方式を採用することにより、第1の利用者から第2の利用者にキー情報を複製させる場合にロックさせることが可能となる。

【0076】

第2の利用者は、第1の利用者から複写したデジタル情報158を再生しようとしてもキー情報160にロック情報161が付加されているため、そのまま再生することはできない。ここで、第2の利用者がデジタル情報158を再生

するためにはデジタル情報販売元 1 5 0 又はサポートセンタ 1 5 1 へのアクセスが必要とする。

【 0 0 7 7 】

図 1 6 のフローチャートを用いて、第 2 の利用者が料金を支払い、デジタル情報 1 5 7 を再生する方法について説明する。

【 0 0 7 8 】

利用者カード制御装置 1 (カードスロットなど) に先に複写したロック状態のキー情報が格納される第 2 利用者の記憶媒体 (IC カードなど) が装着されると、デジタル情報制御装置 1 3 の利用者ユニット制御手段 (PC など) の制御により利用者カード制御装置 1 経由でキー情報を取得する。このキー情報のサポートセンターへの送信は利用者外部通信手段 2 3 (モデムなど) により回線 (電話回線など) を経由して行う。

【 0 0 7 9 】

サポートセンターでは受信したキー情報が同センターでサポート可能であることを判別した後、可能であれば、キー情報より取得した料金を請求することを示す情報を上記回線経由で送信する。次に第 2 利用者側では請求された金額情報をサポートセンターへ送金する。この金額情報をサポートセンターで受け取った後、受領を意味する領収情報を送信する。続いてサポートセンターでは先に受信した第 2 利用者からのロック状態のキー情報に対してロックを解除する処理を行う。このロック解除ではデジタル情報の販売元固有のコードによりキー情報の値を演算することが唯一ロック状態を示すデータを変更できるアルゴリズムとなっている。ロック解除の処理が完了するとキー情報をサポートセンター側から第 2 利用者側へ送信する。また、回線経由で送信されるキー情報には暗号化処理が施されているため、キー情報送信に使用する回線上で同キー情報が盗聴して使用を試みてもそのままの使用はできないことになっている。上記の手順で料金の支払いとロック状態を解除されたキー情報を受信した第 2 利用者はこのキー情報によりデジタル情報を再生する。

【 0 0 8 0 】

次に、図 1 7 のフローチャートを用いて、第 2 の利用者が料金を支払い、ディ

デジタル情報 1 5 7 を再生する他の方法について説明する。

図 1 7 のフローチャートは、図 1 6 のフローチャートと、サポートセンターで行うキー情報に対しロック解除の処理と料金徴収処理の順番が異なる。

【 0 0 8 1 】

第 2 次利用者がサポートセンターにアクセスし、キー情報を送信する。キー情報を受信したサポートセンタは、キー情報を判別し、キー情報のロック解除を開始する。ロック解除が完了した後、請求情報を転送する。

【 0 0 8 2 】

第 2 次利用者が代金を送金し、決済が完了すると、サポートセンタが涼秋情報と、ロック解除のためのキー情報を送信する。

【 0 0 8 3 】

図 1 6 と図 1 7 では、ロック解除の処理と料金徴収処理の順番が異なるために、エラー発生またはロック解除キャンセル時の処理が異なる。図 1 6 ではキー情報のロック解除処理を代金受領の後に行うため、利用者の要求でロック解除キャンセルとなった場合にロック解除処理を行わずに済むため、サポートセンターとしては不要な処理が発生しない形態となる。図 1 7 では、前もってロック解除の処理を行うことで、代金受領後に処理したキー情報を素早く送信できるため、利用者の待ち時間が減少する。また、代金受領後の回線切断により利用者へキー情報を送信できない確率が低くなる。

【 0 0 8 4 】

なお、支払は現金決済でも良いし、電子マネー決済でも良い。また、キー情報はデジタル情報個々に異なるものなので、複数のデジタル情報を利用する場合、各キー情報に対して販売元エリアの電子マネーを個別に格納すると購入料金回収先となる販売元を区別したり、振り込みなどの処理を行う際、利便性が向上する。

【 0 0 8 5 】

さらに、複数のキー情報を格納することで、上記キー情報 1 3 7 を格納するメモリの容量が不足した場合、その旨を利用者に通知して、不必要なキー情報を消去できるようにしても良い。また、上記複写の開始時に、“複写は有料”である

ことを利用者へ知らせることは必要なガイダンスの1つであり、通知の形態は問わないが必ず行う。

【0086】

また、図示しないがサポートセンタ131に支払われた利用者からの購入料金はオンラインでリアルタイムにデジタル情報販売元130へ送金することにしても良い。

【0087】

方法により第3、第4とデジタル情報のコピーが利用者間で行われても、コピー実行時には販売元が回収可能な金額情報が生成され、再生時の利用者のアクセスにより、必ず販売元へデジタル情報に対する購入料金が回収できることになり、利用者間における複製行動を利用した拡販が期待できるため、販売者と利用者の直接販売と異なる形態（利用者間の口コミ販売のようなもの）には、効果的な方法となる。

【0088】

本実施例においては、デジタル情報154、158と、キー情報156、160を同じ記憶媒体153、157に記憶させる例を説明したが、第1の実施例と同様に、別々の媒体に記憶させてもよい。また、第1の実施例と同様に、キー情報を利用者固有の秘密かぎ情報により暗号化することにより、利用者情報に関連した暗号化情報を利用してこととなるので、利用者間の複製に対して安全性の高いデジタル情報の販売システムとなる。なお、本実施例におけるキー情報の複製の制御やキー情報のロック解除制御は、販売元等から配信、提供されたキー情報制御プログラムに規定されており、このキー情報制御プログラムは、キー情報の複製と共に、それぞれの利用者記憶媒体等に記憶される。

【0089】

なお、キー情報を使用不可の状態で複製させる本実施例は、第2の利用者へのキー情報複製を禁止する構成と比べて、セキュリティを高くすることができる。例えば、第2の利用者へのキー情報複製を禁止し、キー情報をアクセスにより手に入れる方法では、1種類のデジタル情報（例えば、ある映画1本、ある音楽1曲）については、同じ1つのキー情報を使用しなくてはならない。このような

方式では、あるキー情報が解読されてしまうと、多数の人間がそのデジタル情報を複合化して使用できるため、セキュリティが低くなってしまう。キー情報を使用不可の状態で複製させる本実施例においては、1種類のデジタル情報について、複数のキー情報を割り当てることができる。複数のキー情報を割り当てても、複製されたキー情報をサポートセンターに送信することにより、キー情報をセンターで照会できるからである。従って、1種類のデジタル情報（例えば、ある映画1本、ある音楽1曲）に複数のキー情報を割り当てた場合は、1つのキー情報が解読されたからといって、その他のキー情報を持つデジタル情報は使用できないため、セキュリティを高くすることができる。

【0090】

以上のように本実施例では、利用者間で複製されたデジタル情報の利用時には、必ず利用者による販売元へのアクセスを必要とする方式としているので、販売元は確実にデジタル情報の利用に対する料金を回収できることになる。この方式によれば、ネットワークに接続された再生端末を所有する利用者間のデジタル情報の複製を管理可能であり、利用者からの要求によりリアルタイムでデジタル情報の利用を許可にしたり、また、その料金を回収することができることとなる。

【0091】

【発明の効果】

本発明によれば、デジタル情報の販売、配信に際して、利用者間の不正な複製を防止でき、料金を回収できるという効果が得られる。

【図面の簡単な説明】

【図1】

本発明の一実施例のシステム構成1を示す図である。

【図2】

本発明の一実施例のデジタル情報販売手順を示すフローチャートである。

【図3】

本発明の一実施例のデジタル情報再生手順を示すフローチャートである。

【図 4】

本発明の一実施例のデジタル情報転売手順を示すフローチャートである。

【図 5】

本発明の一実施例の I C カードの構成 1 を示す図である。

【図 6】

本発明の一実施例の利用者間を移動する情報の流れを示す図である。

【図 7】

本発明の一実施例の利用者間の料金回収手順 1 を示すフローチャートである。

【図 8】

本発明の一実施例のシステムの構成 2 を示す図である。

【図 9】

本発明の一実施例の I C カードの構成 2 を示す図である。

【図 1 0】

本発明の一実施例の利用者間の料金回収手順 2 を示すフローチャートである。

【図 1 1】

本発明の一実施例の利用者間の料金回収手順 3 を示すフローチャートである。

【図 1 2】

本発明の一実施例のシステムの構成を示す図である。

【図 1 3】

本発明の一実施例の銀行 A T M の回収手順 1 を示すフローチャートである。

【図 1 4】

本発明の一実施例の銀行 A T M の回収手順 2 を示すフローチャートである。

【図 1 5】

本発明の一実施例のシステムの構成を示す図である。

【図 1 6】

本発明の一実施例の料金の回収手順を示すフローチャートである。

【図 1 7】

本発明の一実施例の料金の回収手順を示すフローチャートである。

【符号の説明】

- 1 デジタル情報販売装置
- 2 デジタル情報
- 3 暗号化情報生成器
- 4 販売元所有の I C カード
- 5 販売元所有 I C カード制御装置
- 6 利用者所有の I C カード
- 6 - 1 第 1 利用者の I C カード
- 6 - 2 第 2 利用者の I C カード
- 7 利用者所有 I C カード制御装置
- 8 販売履歴メモリ
- 9 販売社外部通信手段
- 1 0 販売元プログラム格納メモリ
- 1 1 販売者側外部入出力手段
- 1 2 販売者ユニット制御手段
- 1 3 デジタル情報制御装置
- 1 4 暗号化情報再生器
- 1 5 利用者カード制御装置 1
- 1 6 利用者カード制御装置 2
- 1 7 デジタル情報格納媒体制御装置
- 1 8 利用者側プログラム格納メモリ
- 1 9 利用者側プログラム制御手段
- 2 0 デジタル情報再生手段
- 2 1 利用者側入出力手段
- 2 2 利用者ユニット制御手段
- 2 3 利用者側外部通信手段
- 3 0 I / O (I C カードインタフェース信号入出力部)
- 3 1 履歴格納メモリ
- 3 2 暗号 / 復号化手段

- 3 3 メモリ
- 3 4 キー管理メモリ
- 3 4 - 1 第 1 利用者キー情報格納エリア
- 3 4 - 2 販売者キー格納情報エリア
- 3 5 ロック管理メモリ
- 3 5 - 1 第 1 利用者ロック情報格納エリア
- 3 6 電子マネー格納メモリ
- 3 6 - 1 第 1 利用者専用エリア
- 3 6 - 2 販売元専用エリア
- 3 8 演算手段
- 3 9 アクセス管理手段
- 4 0 I / O (I C カードインタフェース信号入出力部)
- 4 1 履歴格納メモリ
- 4 2 暗号 / 復号化手段
- 4 3 メモリ
- 4 4 キー管理メモリ
- 4 4 - 1 第 2 利用者キー情報格納エリア
- 4 4 - 2 販売者キー格納情報エリア
- 4 5 ロック管理メモリ
- 4 5 - 1 第 2 利用者ロック情報格納エリア
- 4 6 電子マネー格納メモリ
- 4 6 - 1 第 2 利用者専用エリア
- 4 6 - 2 販売元専用エリア
- 4 8 演算手段
- 4 9 アクセス管理手段
- 5 0 デジタル情報販売店
- 5 1 デジタル情報
- 5 2 販売元固有の暗号化情報
- 5 3 販売元固有の秘密かぎ情報

5 4	販売者所有の I C カード
5 5	暗号化されたデジタル情報
6 0	第 1 利用者オンライン端末
6 1	第 1 利用者固有の秘密かぎ情報
6 2	第 1 利用者固有の暗号化情報
6 3	第 1 利用者の I C カード
6 4	第 1 利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ 情報
7 0	第 2 利用者オフライン端末
7 1	第 2 利用者固有の秘密かぎ情報
7 2	第 2 利用者固有の暗号化情報
7 3	第 2 利用者の I C カード
7 4	第 2 利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ 情報
8 0	第 3 利用者オフライン端末
8 1	第 3 利用者固有の秘密かぎ情報
8 2	第 3 利用者固有の暗号化情報
8 3	第 3 利用者の I C カード
8 4	第 3 利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ 情報
9 0	第 N 利用者オンライン端末
9 1	第 N 利用者固有の秘密かぎ情報
9 2	第 N 利用者固有の暗号化情報
9 3	第 N 利用者の I C カード
9 4	第 N 利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ 情報
1 0 0	販売元
1 0 1	第 1 利用者オンライン環境下の端末
1 0 2	第 2 利用者オフライン環境下の端末

- 1 0 3 第 3 利用者オフライン環境下の端末
- 1 0 4 第 4 利用者オンライン環境下の端末
- 1 0 5 第 5 利用者オフライン環境下の端末
- 1 0 6 第 6 利用者オフライン環境下の端末
- 1 0 7 第 7 利用者オフライン環境下の端末
- 1 0 8 第 8 利用者オンライン環境下の端末
- 1 0 9 第 n 利用者オンライン環境下の端末
- 1 1 0 回線
- 1 2 0 演算手段
- 1 2 1 I / O (I C カードインタフェース信号入出力部)
- 1 2 2 暗号 / 復号化手段
- 1 2 3 制御プログラム格納メモリ
- 1 2 4 プロバイダ契約情報格納メモリ
- 1 2 5 履歴格納メモリ
- 1 2 6 電子マネー格納メモリ
- 1 2 6 - 1 第 1 利用者専用エリア
- 1 2 6 - 2 販売元専用エリア
- 1 2 7 アクセス管理手段
- 1 2 8 ロック管理メモリ
- 1 2 8 - 1 第 1 利用者ロック情報格納エリア
- 1 2 9 キー管理メモリ
- 1 2 9 - 1 第 2 利用者キー情報格納エリア
- 1 2 9 - 2 販売者キー格納情報エリア
- 1 4 0 デジタル映像販売元
- 1 4 1 銀行 A T M
- 1 4 2 利用者 1 の金額情報格納エリア
- 1 4 2 - 1 利用者 1 の利用者専用エリア
- 1 4 2 - 2 利用者 1 の販売元専用エリア
- 1 4 3 利用者 1 のアプリケーション格納メモリ

- 144 キー管理メモリ
- 145 デジタル映像情報
- 146 利用者2のアプリケーション格納メモリ
- 147 利用者2の金額情報格納エリア
- 147-1 利用者2の利用者専用エリア
- 147-2 利用者2の販売元専用エリア
- 150 デジタル情報提供元
- 151 サポートセンタ
- 153 第1の利用者の記憶媒体
- 157 第2の利用者2の記憶媒体
- 160 デジタル情報利用のためのキー情報
- 161 デジタル情報利用のためのキー情報のロック情報

【書類名】 図面

【図 1】

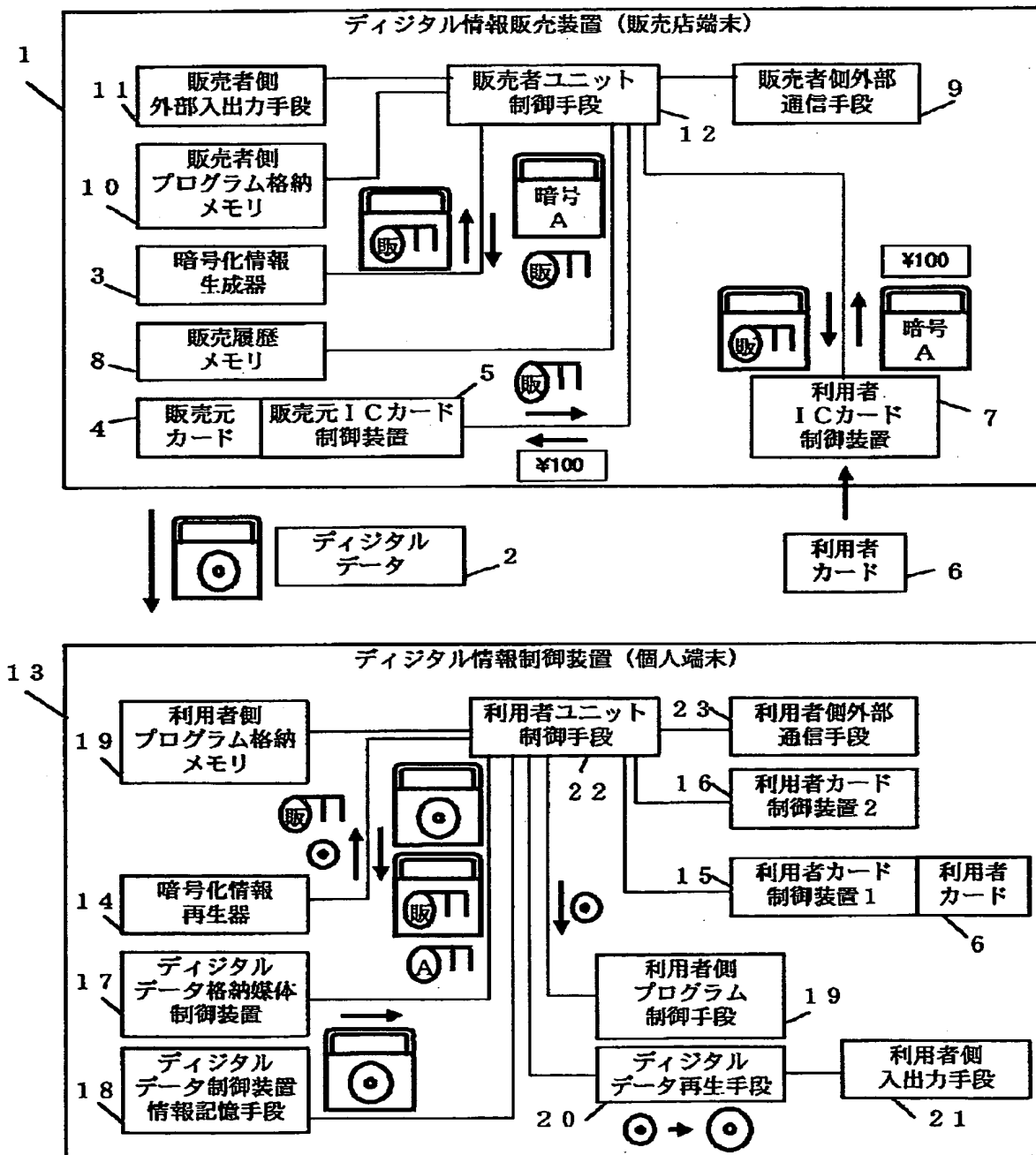


図 1

【図 2】

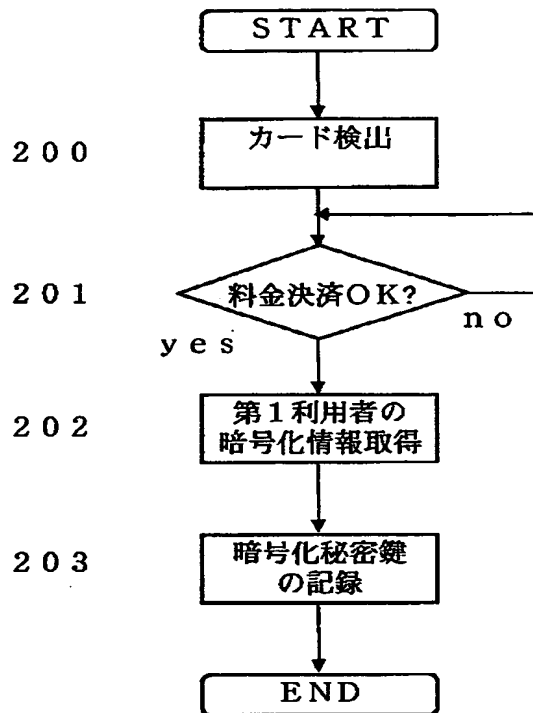


図 2

【図 3】

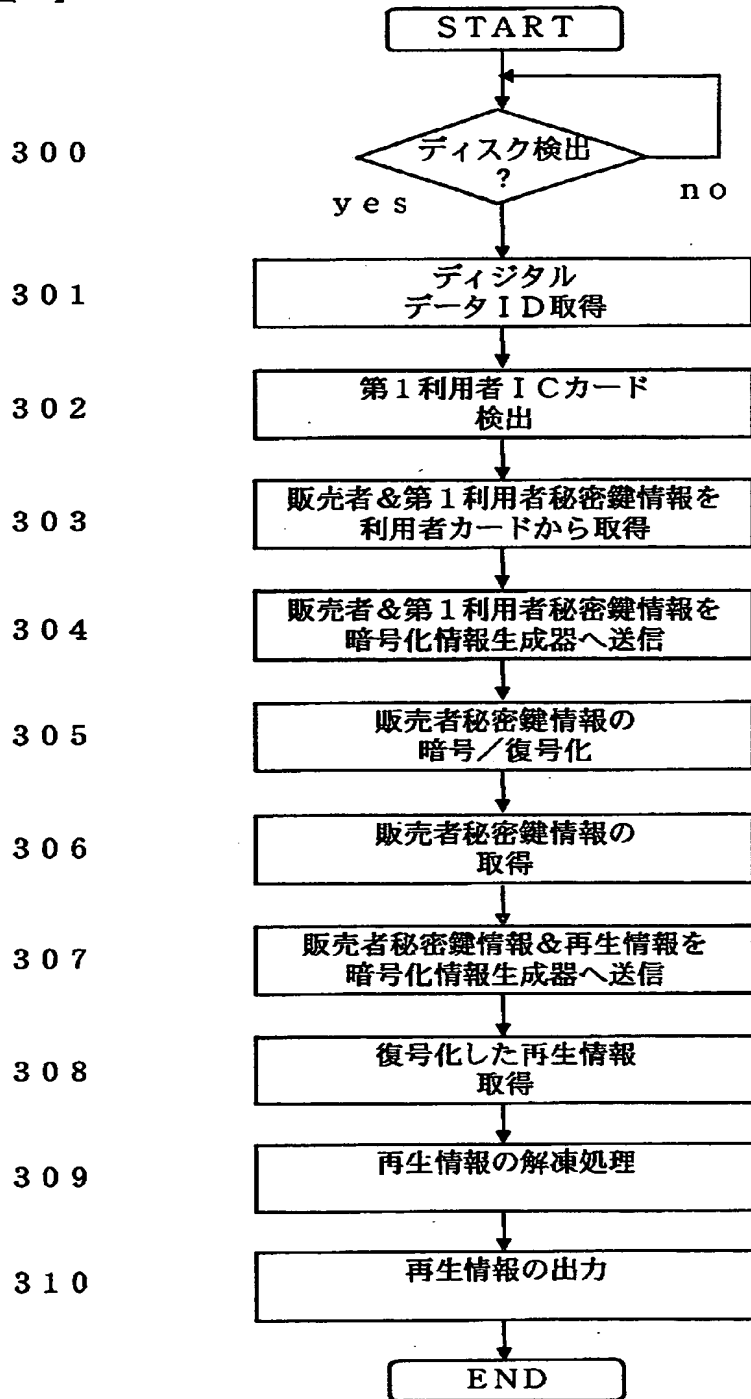


図 3

【図4】

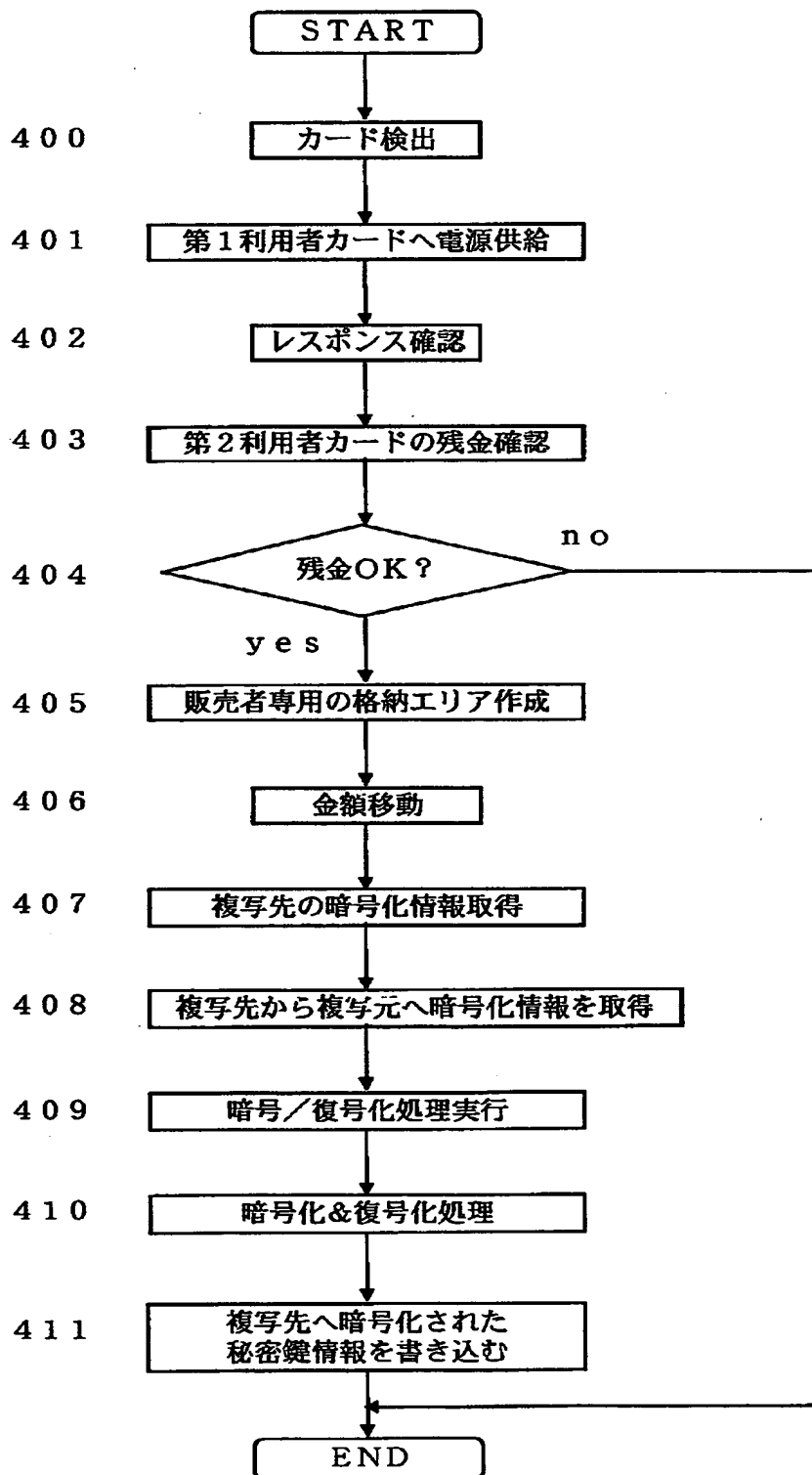


図4

【図5】

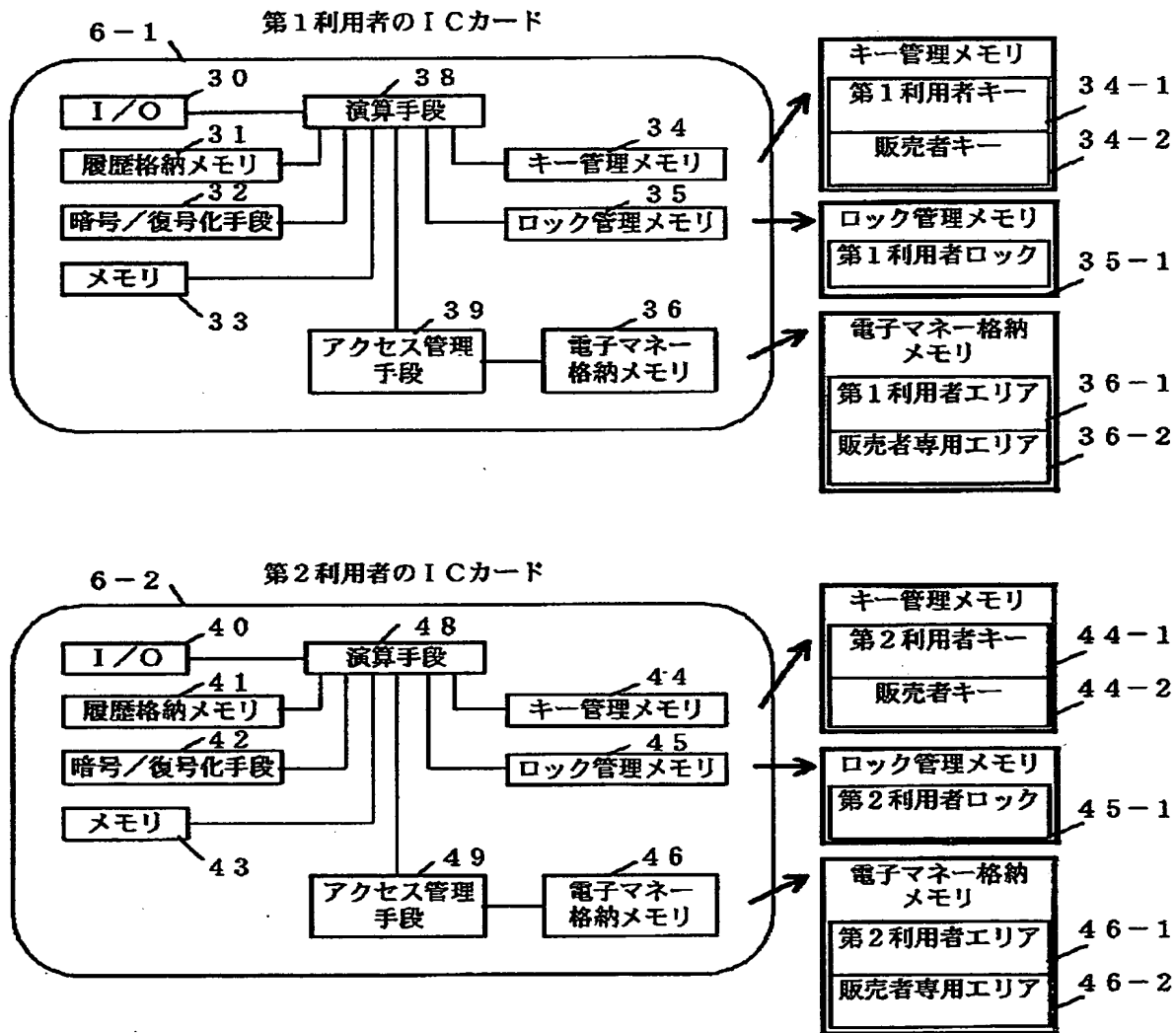


図5

【図 6】

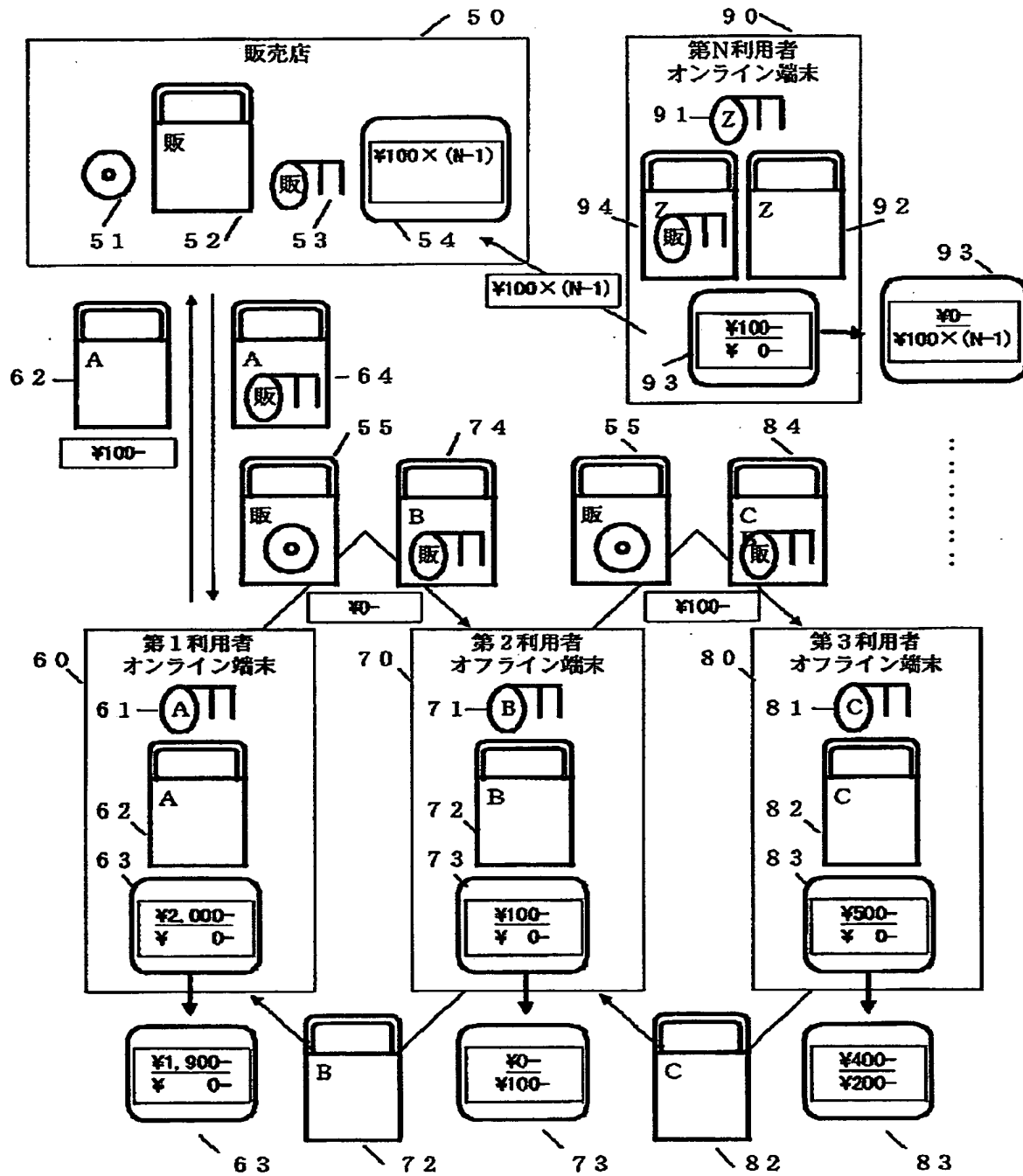


图 6

【図 7】

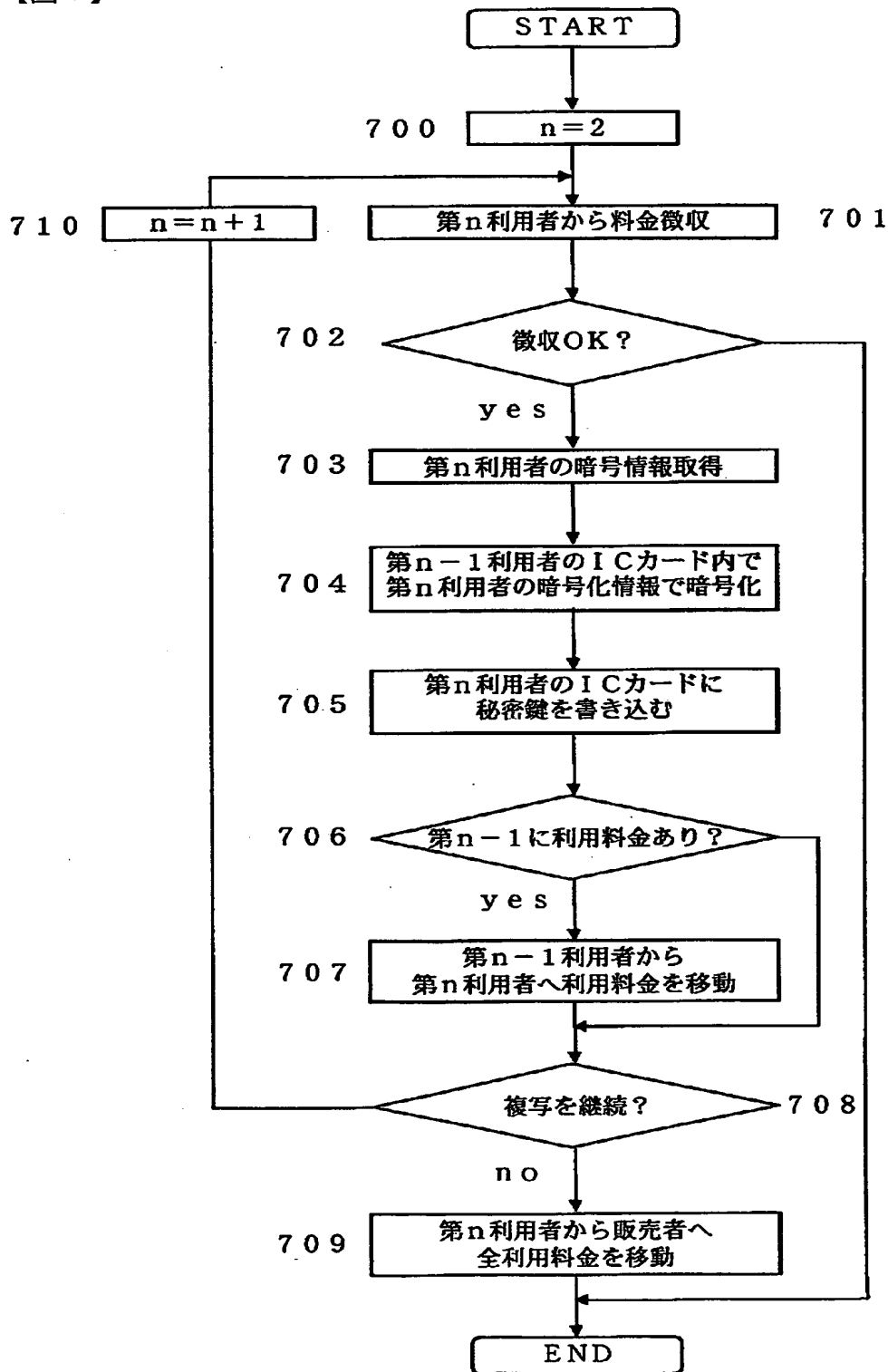


図 7

【図 8】

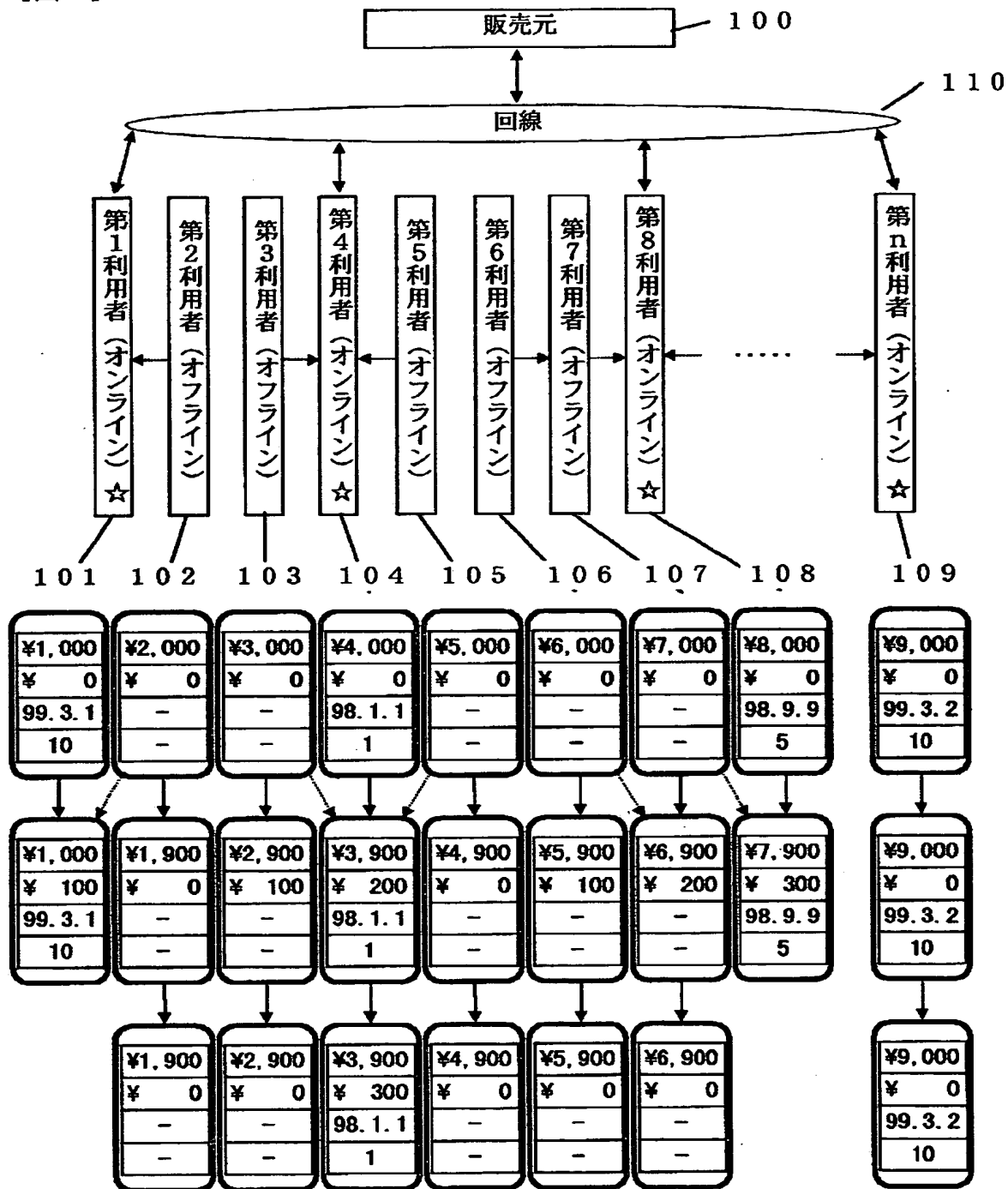


図 8

【図9】

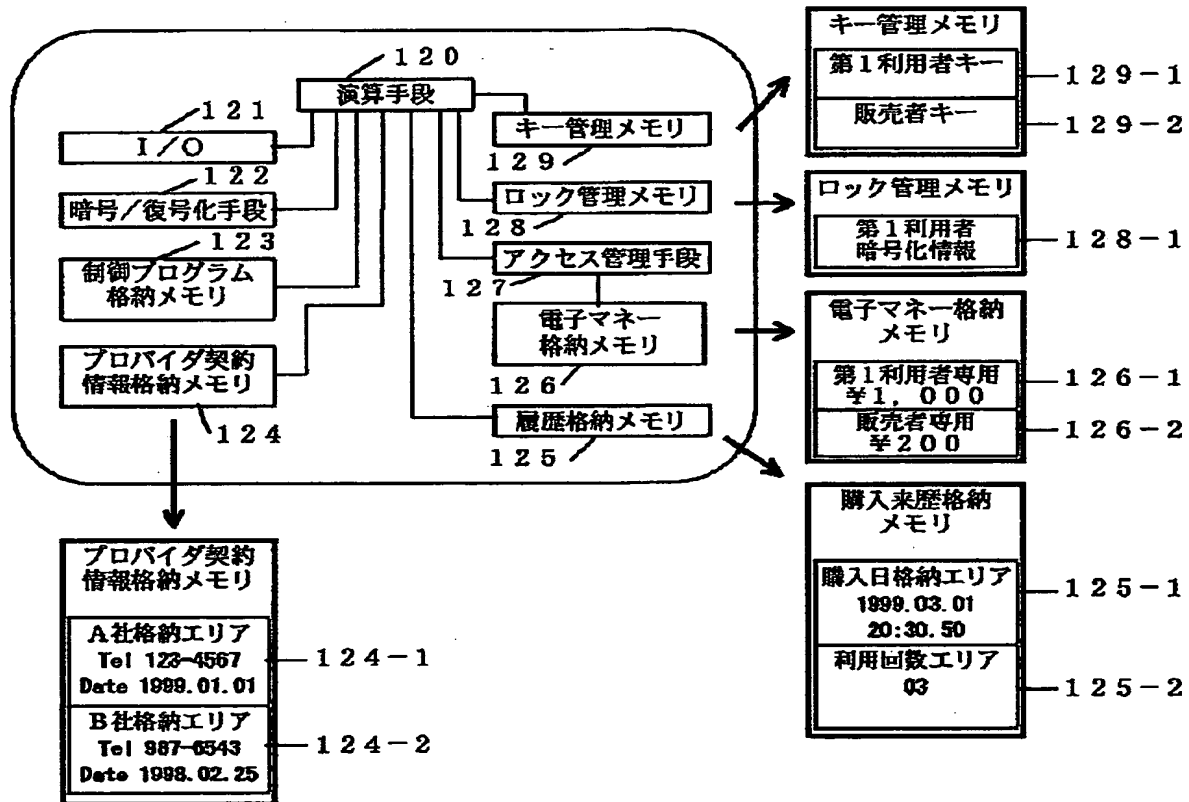


図9

【図10】

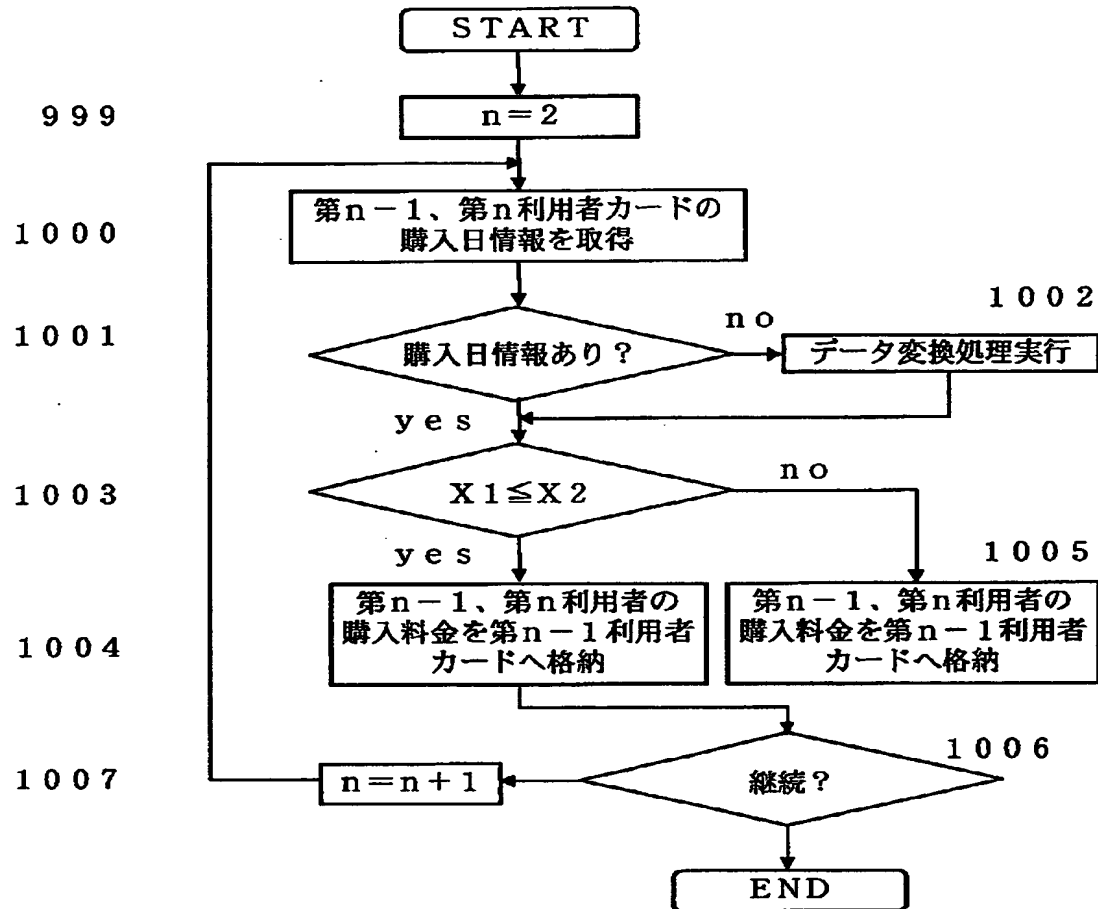


図10

【図11】

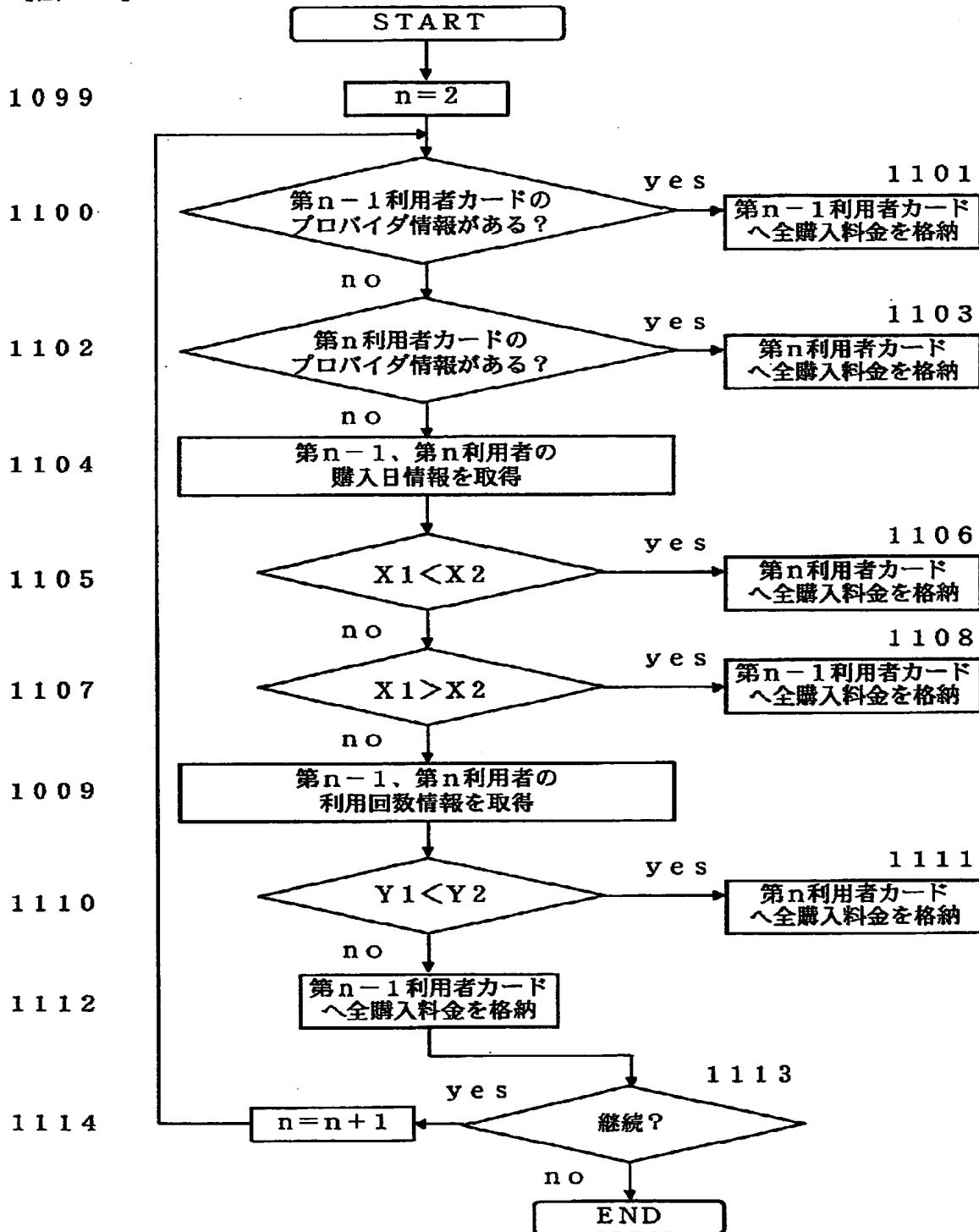


図11

【図12】

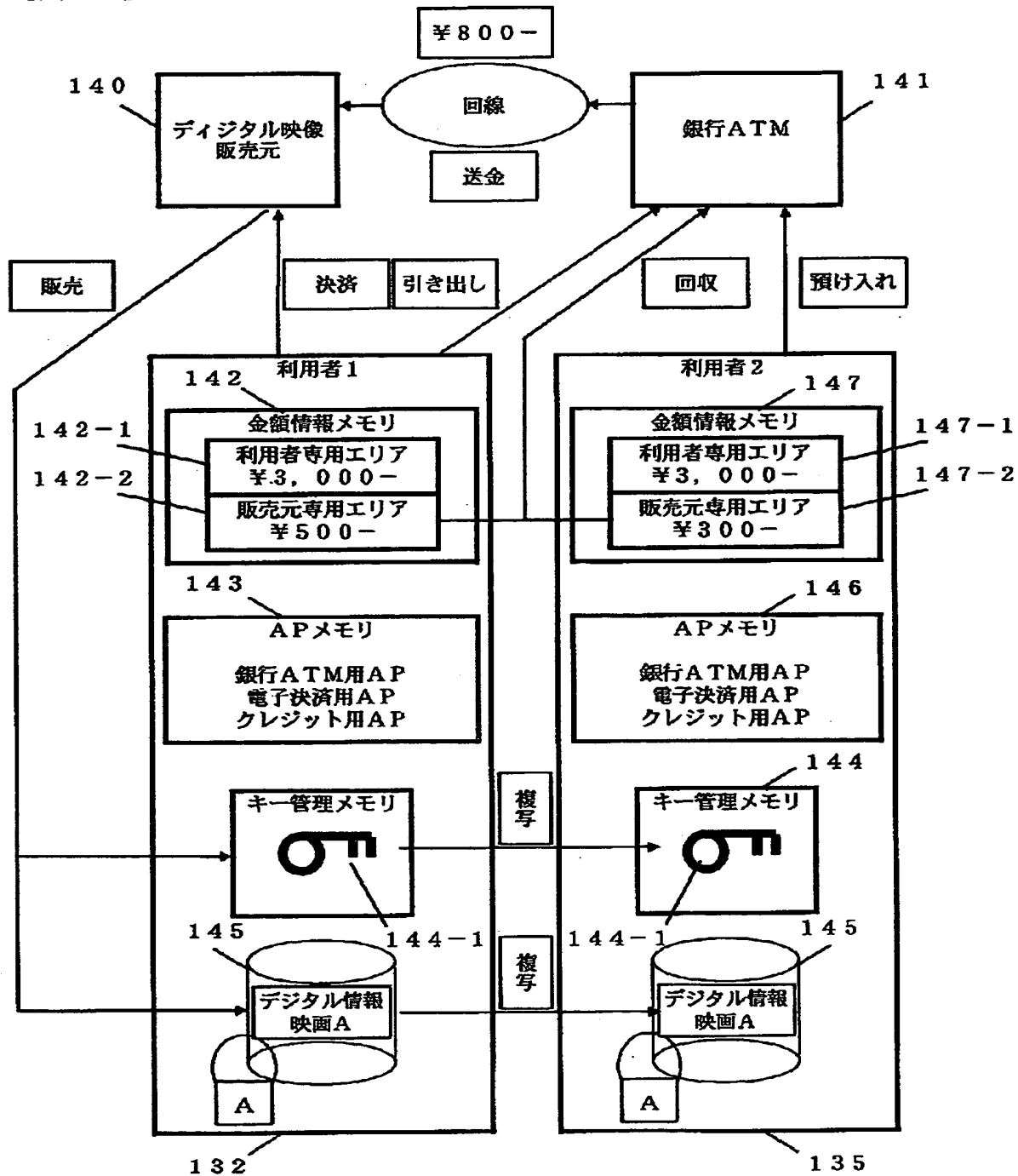


図12

【図 1 3】

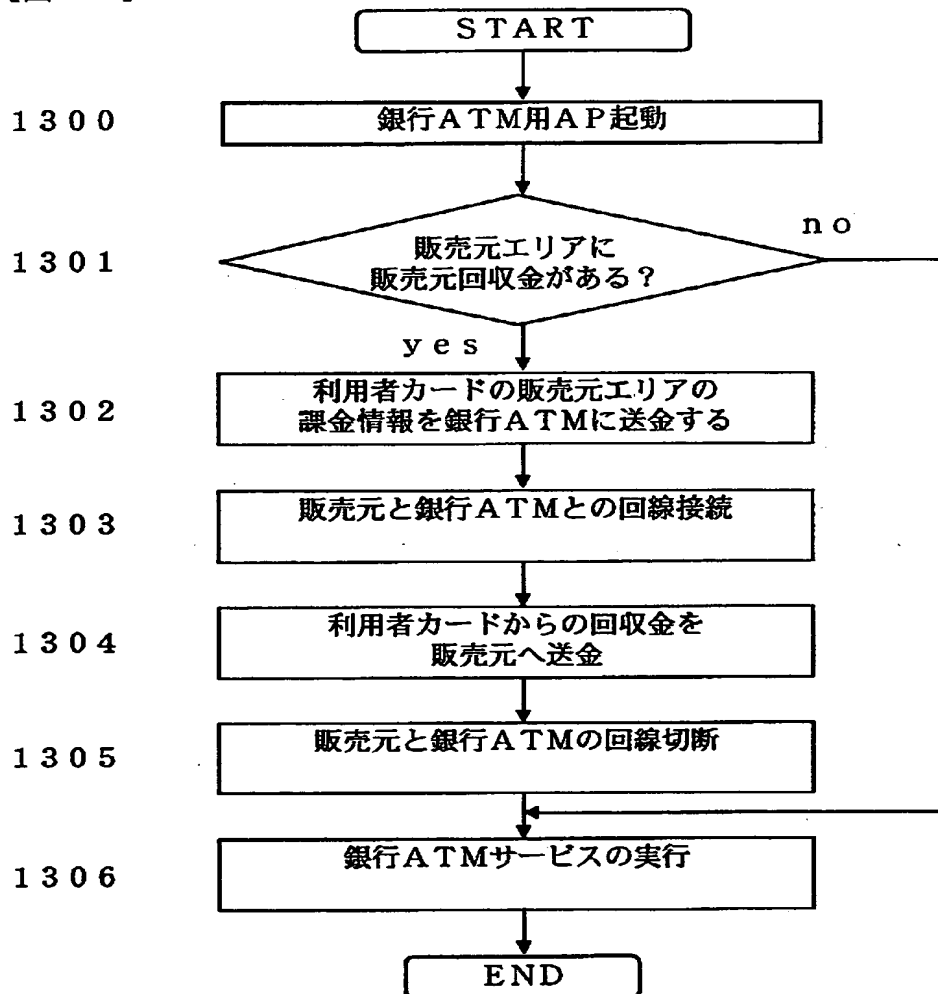


図 1 3

【図 1 4】

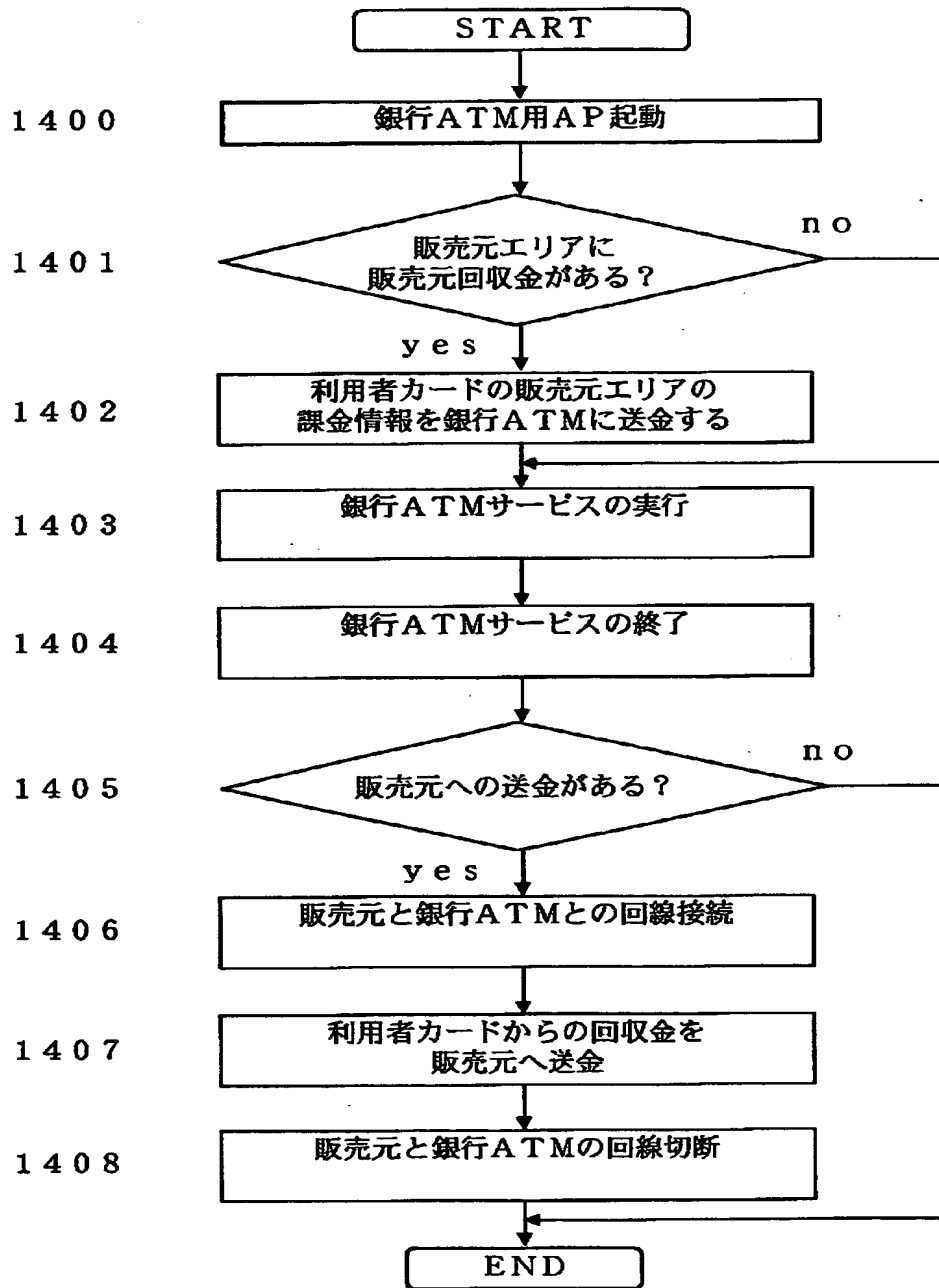


図 1 4

【図 1 5】

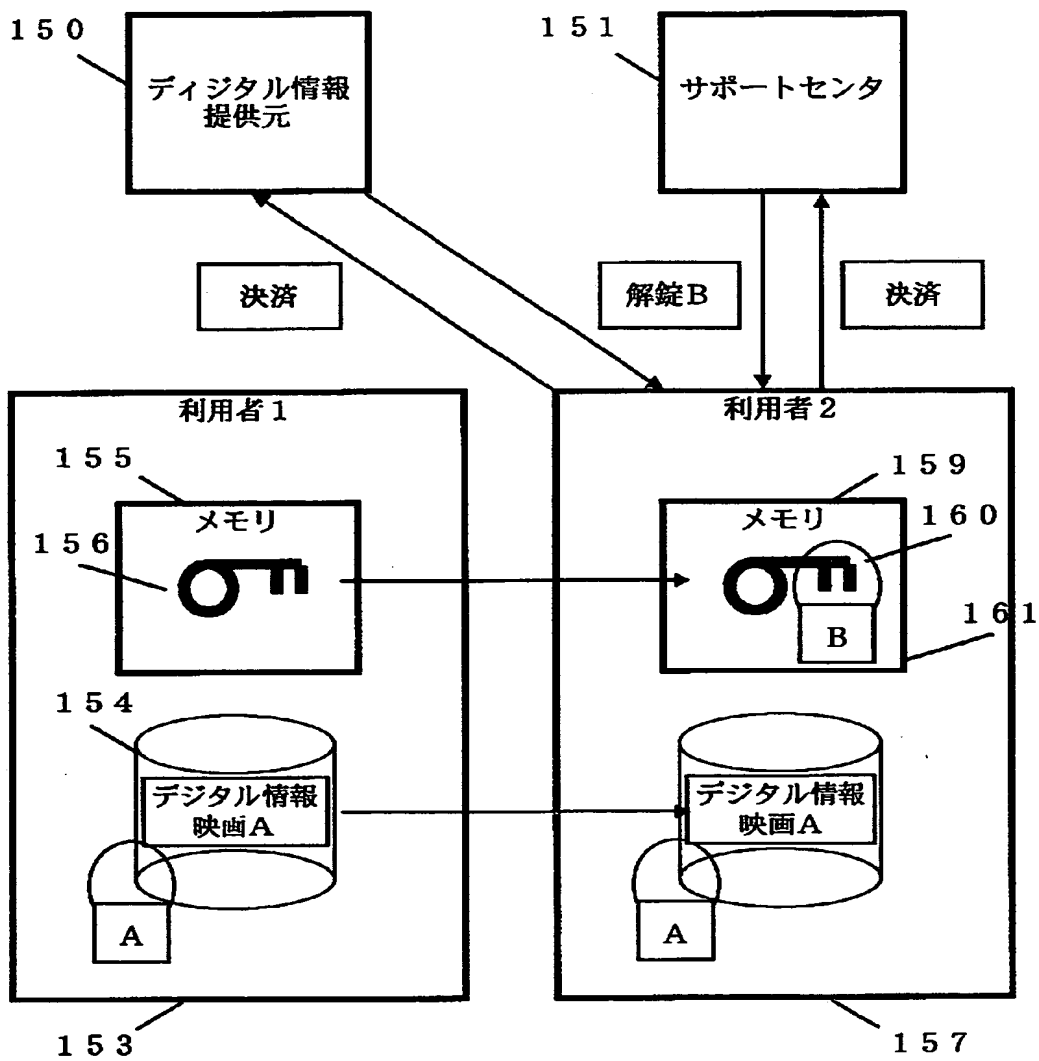
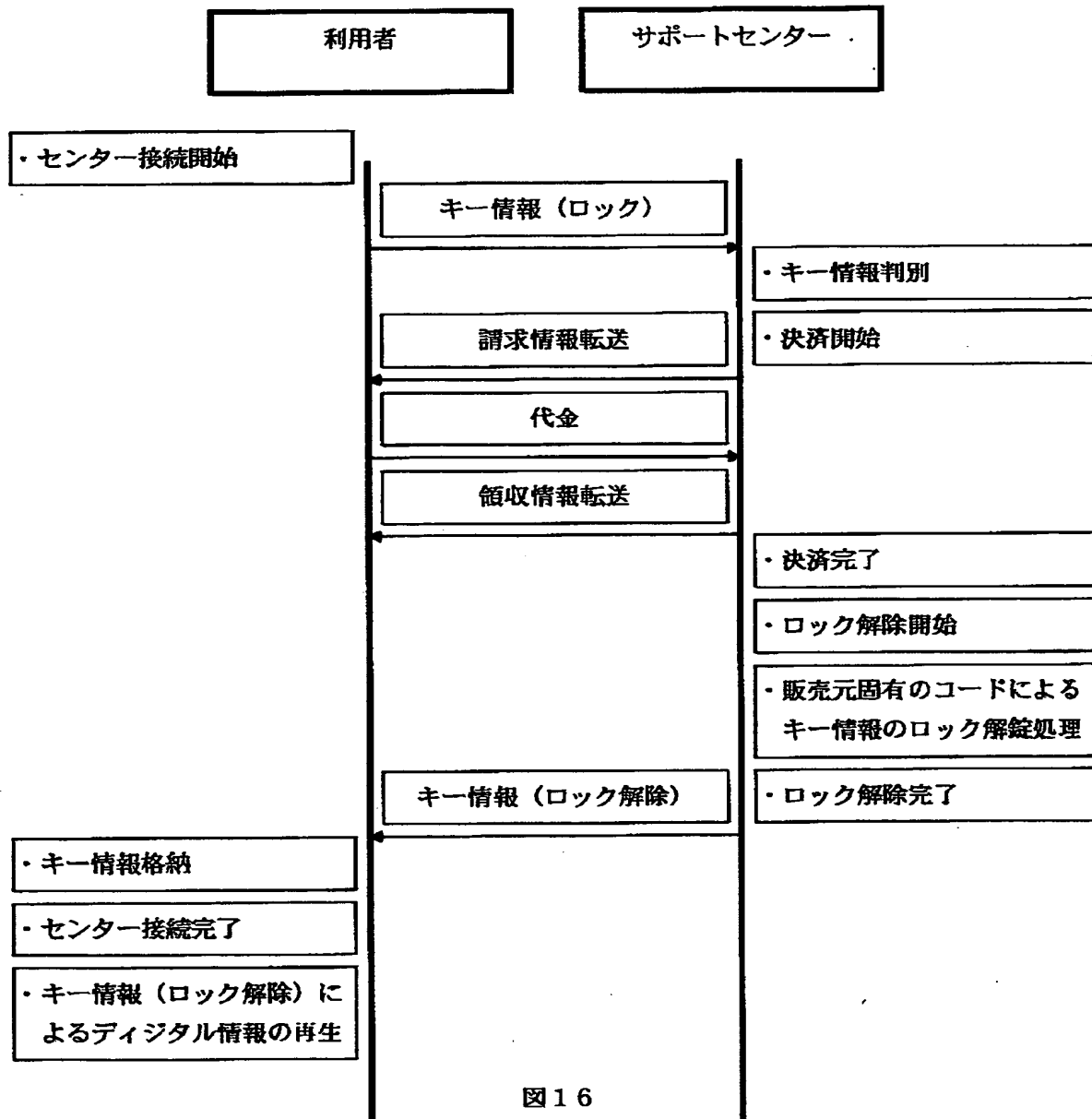


図 1 5

【図 16】



【図 17】

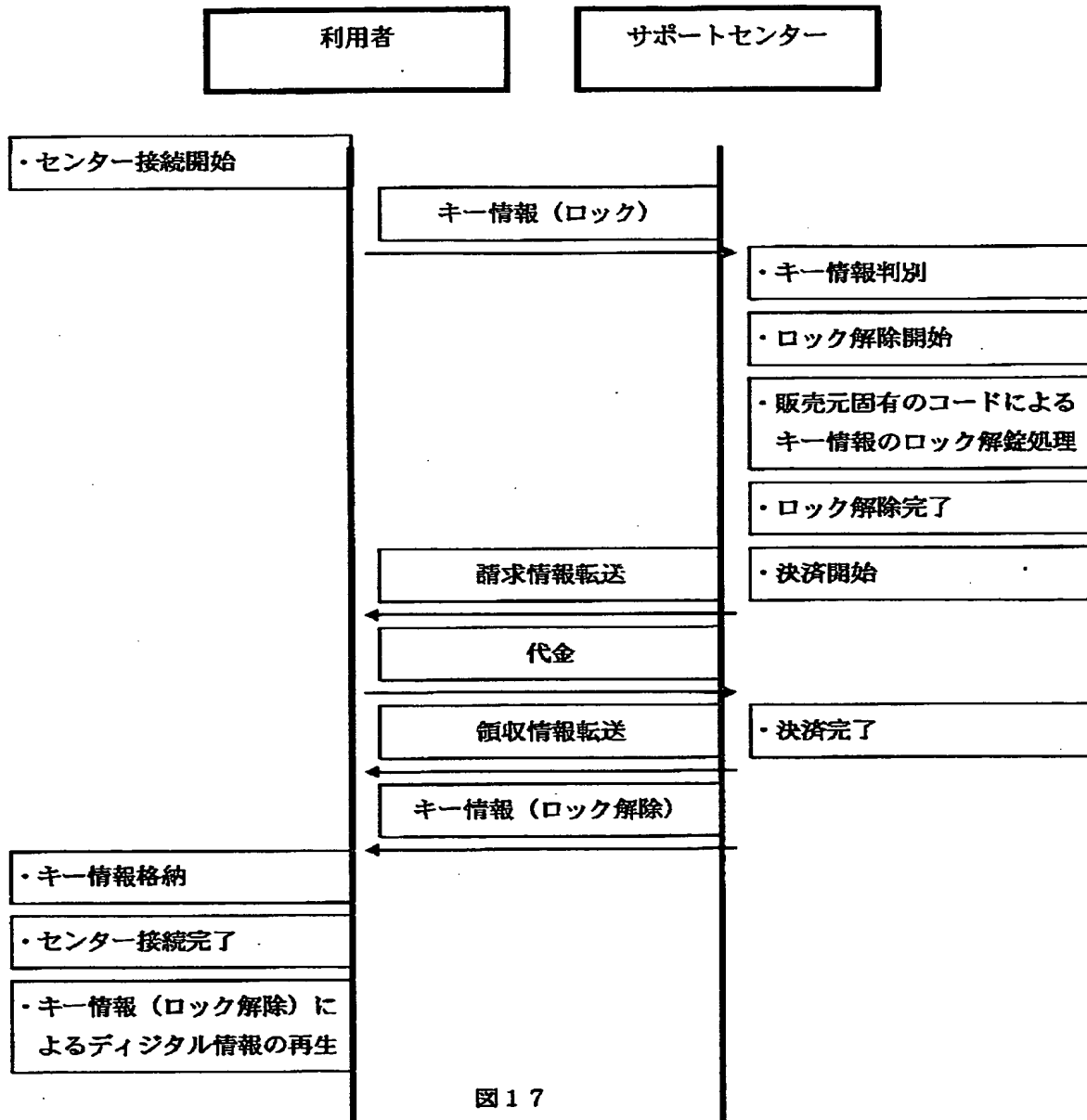


図 17

【書類名】 要約書

【要約】

【課題】

デジタル化された映像、音楽、著書などのデジタル情報に対する不正な複製を防止し、複製したデジタル情報の利用に伴う料金をデジタル情報の権利者へ確実に回収できる方法を提供する。

【解決手段】

デジタル情報158の利用許可を行うキー情報156を複製する際には、ロックした状態で複製させ、キー情報156のロックを解除させる際には、販売元150へアクセスすることにより、デジタル情報の利用料金を支払う。

【選択図】 図15

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [000233136]

1. 変更年月日	1991年 4月24日
[変更理由]	名称変更
住 所	神奈川県横浜市戸塚区吉田町292番地
氏 名	株式会社日立画像情報システム